2019

Advancing User Authentication and Access Management

Crume, Jeffery

UNIVERSITY OF PLYMOUTH

Advancing User Authentication and Access Management

by

Jeffery Crume

A thesis submitted to the University of Plymouth in partial fulfilment for the degree of

DOCTOR OF PHILOSOPHY

School of Computing, Electronics and Mathematics

May 2019

COPYRIGHT STATEMENT

TABLE OF CONTENTS

TABLE OF FIGURES

AUTHOR'S DECLARATION

At no time during the registration for the degree of Doctor of Philosophy has the author been registered for any other University award without prior agreement of the Doctoral College Quality Sub-Committee.

Work submitted for this research degree at the University of Plymouth has not formed part of any other degree either at the University of Plymouth or at another establishment.

Word count of the main body of thesis: 14,888

Signed 

Date May 17, 2019

ABSTRACT

Advancing User Authentication and Access Management

Jeffery Lake Crume

In order for online systems to transact business or exchange other sensitive information, there must be an environment where the parties involved can verify that the other is who they claim to be. Authentication mechanisms provide this verification process, thereby, improving confidence in the confidentiality and integrity of communications.

However, attackers can exploit this trust if they are able to successfully impersonate a legitimate user and gain access to the system with all the rights and privileges of that user. One particularly difficult class of attacks of this sort involves an attacker inserting themselves between the end user and the system they are communicating with. This man-in-the-middle (MITM) scenario affords the attacker access to passwords, transaction details and other sensitive information, which they may then modify or use to suit their purposes resulting in identity theft, information compromise and misappropriation of funds via electronic transfer, among other scenarios.

Current solutions are able to mitigate some of this risk, but more work is needed here given the difficulty in detecting MITM attacks. This thesis deals generally with the subject of identity and access management with a specific focus in the area of authentication within an IT system.

The research described here provide new approaches to user-centric and transaction-centric authentication as well as capabilities to improve support for the broader authentication system. The first category of user-centric improvements involves mechanisms which:

- leverage a communications side channel so that the user can know with greater certainty that the website they are interacting with is the one they intend,
- allow a service provider to detect a MITM by determining the user's geographical location is consistent across multiple channels,
- allow for the detection of a MITM through an out of band voice prompt presented to the user and
- improve confidence that a user is who they claim to be by dynamically verifying that they are geographically where they are expected to be even when traveling.

The second category of transaction-centric improvements involves mechanisms which leverage out of band communications to verify transaction details have not been tampered with through:

- a voice call in which transaction amounts, accounts, etc. are read aloud to the user for confirmation and
- a specially constructed QR code which contains these details and can be verified with a purpose-built mobile app.

The third category of broader authentication system support mechanisms which:

- detect a MITM attack by recognizing changes in login traffic patterns,
- detect rogue domain name service providers which might attempt to redirect traffic to attacker websites,
- allow for non-disruptive, secure migration of users across authentication systems and
- allow for a secure means to regain access to a mobile device for which the passcode has been lost.

This research consists of a body of published works, most of which have taken the form of patent filings, which have been peer reviewed and granted by the US Patent and Trademark Office.

GLOSSARY OF ABBREVIATIONS

ARP	Address Resolution Protocol
DNS	Domain Name System
IAM	Identity and Access Management
ISP	Internet Service Provider
CA	Certificate Authority
CBK	Common Body of Knowledge
CISSP	Certified Information Systems Security Professional
DOS	Denial of Service
GPS	Global Positioning Systems
HTTPS	Hyper Text Transfer Protocol Secure
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
MITB	Man-in-the-Browser
MITM	Man-in-the-Middle
OOB	Out of Band
OSI	Open Systems Interconnection
OTP	One Time Password
PIN	Personal Identification Number
QR code	Quick Response code
SSL	Secure Sockets Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
USPTO	US Patent and Trademark Office
VRU	Voice Response Unit
Wi-Fi	Wireless Fidelity

1 INTRODUCTION

Fundamental to any important transaction is the notion that the parties to that transaction are, in fact, who they claim to be. Without this assurance, no trust can be established and sensitive information cannot be safely transmitted or business conducted. The process by which this assurance is provided is one of *authentication*.

Authenticating parties in face-to-face settings may involve recognizing the appearance, voice or other biometric considered unique to the parties. Absent this level of prior knowledge for comparison, a system of credentials issued by a trusted third party (e.g. passport, driver's license, etc.) may suffice to establish identity.

However, this process becomes more complex when communications are conducted remotely over a data network. In this case we need to develop other means for authentication. Attackers often exploit this complexity and use it to subvert the system. Therefore, mechanisms for authenticating identities through technical means are needed. Typically, these involve verifying something the individual:

- Knows (e.g. a password, PIN, etc.)
- Has (e.g. a smartcard, mobile phone, security token, etc.)
- Is (e.g. a biometric such as a fingerprint, facial scan, voiceprint, etc.)

1.1 PASSWORD CHALLENGES

Passwords, and other knowledge-based authentication systems, are notoriously weak due, in large part, to the human element involved. Stated in grossly oversimplified terms for effect -- *If a password can be easily remembered, it can be easily guessed.* Conversely, if a password cannot be guessed, it will likely be difficult to remember and will, therefore, result in denying access to authorized users. This is due to the fact that people tend to remember things that are significant or have specific meaning to them such as the name of a pet, a favorite destination, birthdate, spouse's name, etc. (Crume, 2000)

It follows, then, that the more an attacker knows about the personal life and preferences of a user, the greater their odds of being able to guess that user's password. Password cracking tools such as IBM's Cracken (Bryan & Heywood, 2017) are able to process billions of combinations per second in an offline attack (Bryan & Heywood, 2018) and may find shortcuts by using dictionaries of common passwords as a starting point to shorten the time to required.[1] (Ur, et al., 2015)

Based upon an analysis of 70 million user-chosen Yahoo! Passwords, (Bonneau, 2012) found that "passwords provide less than 10 bits of security against an online, trawling attack, and only about 20 bits of security against an optimal offline dictionary attack." This research also found that "even proactive efforts to nudge users towards better password choices with graphical feedback" were largely ineffective. Further, (Adams & Sasse, 1999) found that "users forced to comply with password mechanisms incompatible with work practices may produce responses that circumvent the whole procedure."

In addition to user behaviors, (Morris & Thompson, 1979) describes technical problems dating to the 1960's due to weak security in the way passwords were stored on early online systems. A wide range of vulnerabilities have been

[1] Heywood claims the ability to process 500 billion password hashes per second with a Hashcat configuration. (Heywood, 2017)

exploited over the years since in order to obtain large collections of password hashes and even cleartext passwords. The largest example to date of the latter was the 1.4 billion collection of credentials published on the dark web as a single, aggregate database (Thompson, 2017).

1.2 Other Authentication Challenges

Other authentication methods which rely on something the user has (i.e. possession-based authentication) or something the user is (i.e. biometric-based authentication) introduce additional vulnerabilities (O'Gorman, 2003). Mechanisms involving the former are vulnerable to theft or device cloning (Tabassum, 2017) (Mahato, et al., 2014), while the latter can be compromised through a number of different attacks including (Shan, et al., 2008):

- replay of digitized biometric data (Smith, et al., 2015),
- tampering with the biometric reader (Franken, 2007) and
- imitating physical characteristics of the user resulting in a false positive identification (Patel, et al., 2015).

For these reasons, many organizations have adopted a multi-factor approach to authentication which employs a combination of these methods in order to minimize risk by complicating the task of an attacker.

1.3 Attacker Tactics

In addition to these exploits, attackers frequently set up imposter web sites which have the same look and feel as their legitimate counterparts as a way to steal passwords or other sensitive information. They may then direct a user to the imposter site through a phishing email requesting the user to click on a link embedded in the message contents. This link may be obfuscated such that it appears to match the URL for the user's bank, for instance, but actually points to the imposter site.

In still other cases, attackers may actually insert themselves into the communication path between the user and a legitimate site, thereby, becoming a "man-in-the-middle" (MITM) capable of seeing and even modifying all communications between the two parties. In this scenario, communications, say from a banking customer, will first be sent to the MITM who then may read and/or change the contents before forwarding the transmission on to the bank's web site, and vice versa. If the attacker is successful, both the bank and the customer believe they are communicating exclusively with each other when, in fact, all communications are under the direct control of the MITM attacker. Such attacks are categorized and described by the Common Attack Pattern Enumeration and Classification system as CAPEC-94: Man in the Middle Attack (The MITRE Corporation, 2018).

(Wagner & Bryner, 2001) describes an example of such an attack involving subverting the Address Resolution Protocol in order to route traffic to an MITM site. (Callegati, et al., 2009) discuss the means by which an MITM can undermine the security of the HTTPS protocol via ARP poisoning and self-signed certificates. Further, (Conti, et al., 2016) provides a comprehensive survey of MITM attacks along with a categorization scheme based on the OSI model. The insidious nature of these attacks makes them difficult to detect and defeat. Authentication technologies can assist with this task and help to improve trust in online communications so long as the authentication mechanisms are not also subverted by the MITM.

1.4 Limitations with Existing Defenses

As described in (Burkholder, 2002), the TCP/IP protocol is subject to MITM attacks. With the introduction of session encryption technology such as SSL and, later, TLS, this threat was believed to be detectable and, ultimately

preventable. This resulted from the web browser's ability to detect invalid digital certificates and present the user with a warning message recommending that the session be aborted. However, as this paper demonstrates, an improperly implemented or configured client opens a significant window of vulnerability.

In particular, it finds that:

> *"One faulty SSL client implementation, Microsoft's Internet Explorer, allows for transparent SSL MITM attacks when the attacker has any CA-signed certificate. An even greater risk is posed by unprotected systems where an attacker can preload his/her own trusted root authority certificates. In public environments such as libraries and computer labs, there is little to prevent such an attack from taking place. Casual observation of such places indicates that an attacker would see them as low-risk, high-opportunity environments."*

While the vulnerabilities described are no longer an issue as the particular web browser in question has since been replaced, such a finding can be abstracted and applied to show that encryption protocols and their real-world implementations are not without their problems. The paper goes on to cite other published references such as (Ellison & Schneier, 2000), (Seifried, 2000) and (Seifried, 2000), which provide support for the notion that such vulnerabilities are more prevalent than many would believe and will likely continue to emerge in various forms.

As previously mentioned, an additional problem exists even when all the technical components perform correctly and identify the presence of an imposter web site and that involves the behavior of end users in this scenario. Research conducted by Carnegie Mellon University (Sunshine, et al., 2009) found that 55% and 100% of study participants ignored certificate warning messages regardless of the sensitivity of the material on the site. Another study by Brigham Young University (Jenkins, 2016) found that up to 90% of users studied ignored these warnings while they were multi-tasking. Further, researchers at the University of Pennsylvania and Google (Felt, A.; et al, 2015) found that even a redesigned certificate warning message which conveyed an increased sense of urgency, was essentially ineffective in preventing users from ignoring the message and proceeding in spite of the stated risk.

1.5 Research Aims

This document provides a summary of research upon which the PhD in Information Security will be based. It identifies the nature and significance of these works as they relate broadly to the theme of Identity and Access Management (IAM) and more narrowly to the areas of authentication and authorization.

The objective of this research is to advance the field of Information Security by providing additional mechanisms for authentication and authorization which better detect and defend against impersonation attacks. These attacks may involve a simple case where an unauthorized user attempts to login using stolen credentials. More complex scenarios focus on hijacking sessions between authorized users and legitimate web servers through the insertion of a man-in-the-middle (MITM).

The latter cases may prove particularly difficult to defend against since the MITM may be undetectable by both the user and the web site leading each party to believe that they are dealing directly with the other when, in fact, all communications between the two are subject to review and modification by the eavesdropper. The consequences of such an attack can undermine the entire system of trust necessary for online transactions including e-commerce, banking and others. If left unmitigated, the results could range from compromise of credentials to significant financial loss.

The body of research and publications described here consists of a series of patents – granted and pending – which represent significant, novel contributions to the field. All of the inventions described have been:

1. peer-reviewed by an IBM Invention Disclosure Board comprised of IBM Master Inventors and subject matter experts
2. reviewed by IBM internal legal counsel for prior art conflicts
3. reviewed by external legal counsel for prior art conflicts
4. (for those with patents granted) reviewed and judged to be novel by an independent patent investigator from the United States Patent and Trademark Office (USPTO).

However, it should be noted that while two of the patent filings listed have not as yet been granted, they have, at a minimum, successfully passed through the first three phases of review and judged by IBM, a company that has led the world in patents for more than two decades straight, to be of sufficient novelty and substance to merit a filing with the USPTO.

1.6 Section Structure

Section 2 includes a solution framework which helps address some of the challenges described previously along with a set of integrative use cases, which demonstrate how this research could be deployed in real world examples. Sections 3, 4 and 5 discuss a series of patents which, taken together, provide a set of solutions to the challenges described previously. Specifically, Section 3 focuses on improvements to authenticating users, while Section 4 deals with authenticating transactions. Section 5 complements this work through a discussion of improvements to the overall authentication support system. Section 6 provides a conclusion by summarizing the work and offering areas for future research.

2 SECURITY SOLUTION FRAMEWORK

Given the issues described previously, a solution framework is needed which can reduce risk by creating greater confidence in the authentication system. This problem space is quite complex as evidenced by the substantial body of research that already exists in this area. Still, many of the same fundamental challenges persist in spite of this work.

Identity and access management capabilities should be thought of holistically as part of a larger security solution framework. (Crume, 2014) introduces such a framework along with its key components, as depicted in Figure 1: Identity and Access Management Architecture.

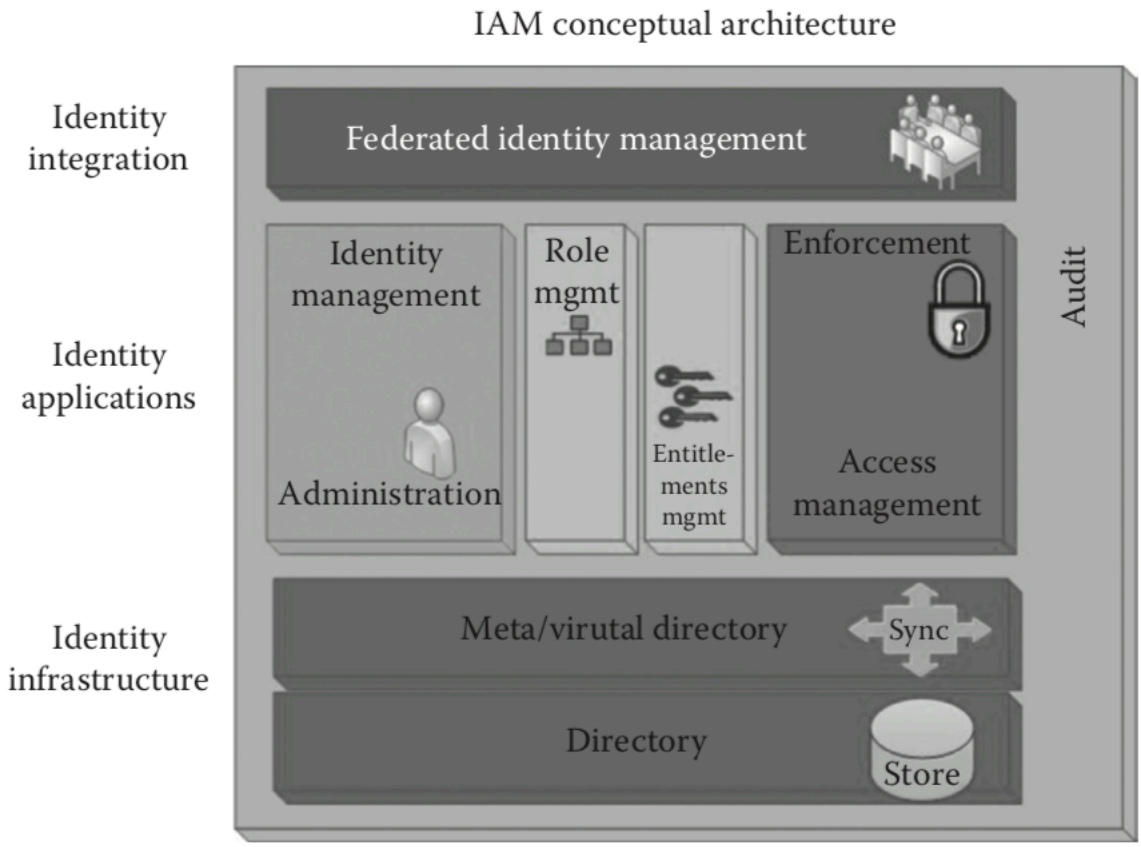


FIGURE 1: IDENTITY AND ACCESS MANAGEMENT ARCHITECTURE

Further, the requirements of the solution framework should include the ability to:

- Verify that the user is who they claim to be.

  This is, of course, the primary requirement of an authentication system. It needs to reject imposters while not putting an undue burden on legitimate users to prove their identities.

- Verify that the user is where they should be, geographically.

A system which knows in advance where a user should be, would be able to deny access to an imposter who might have otherwise been able to fool the system by providing stolen credentials. However, if the system knows, for instance, that the user logging in is not in the location where the legitimate user is scheduled to be, access is denied regardless of whether the credentials are correct. This requirement needs to extend beyond conventional, fixed geographical constraints, which assume that users remain in the same region, and be able to account for global travel for both personal and professional reasons. (Denning & MacDoran, 1998)

- Verify that the web site the user is logging into is not an imposter site.

  Much of the effort spent in the area of authentication focuses on allowing a web site to authenticate a user is who they claim to be. However, given the rise in phishing and other imposter attacks, there is a critical need for users to be able to authenticate that the web site is what it claims to be as well. Server-side certificates help with this but are insufficient since far too many users ignore warning messages when problems are identified. (Sunshine, et al., 2009) (Jenkins, 2016)

- Detect the presence of a rogue DNS resolver attempting to misroute traffic to an imposter site.

  Tremendous faith is placed in the ability of the DNS system to direct network traffic correctly. Most users have no idea how dependent they are on this system, which has been shown repeatedly to be vulnerable to subversion. (Carli, 2003) (Jalalzai, et al., 2015) In order to justify that trust, additional protections are needed to guard against attack.

- Detect the presence of an MITM along the communications path.

  Users implicitly trust that their communications with, for instance, an e-commerce or banking web site are private and cannot be read by anyone other than the organization they intend. In order to ensure that this is the case, there is a requirement to ensure that there are no other parties to these communications, as described by (Callegati, et al., 2009).

- Ensure that transaction details have not been tampered with.

  As with the previous requirement, not only is there a risk of eavesdropping from an MITM reading confidential transmissions, but also with the MITM altering the details of those transactions resulting in substantial losses to the legitimate parties involved. (The MITRE Corporation, 2018)

- Provide a means to ensure that the underlying network has not been subverted.

  One way that attackers are able to hijack sessions is for them to override DNS or other network protocols in order to divert traffic to their MITM as described in (Conti, et al., 2016). The solution needs to detect spoofing of this sort, when possible, and alert support personnel so that appropriate mitigations can be implemented.

- Provide a means for a web site to migrate users to a new authentication system nondisruptively.

  A peripheral requirement for the authentication system would be that it allow for a smooth transition to a replacement system. Typically, such migration of users has resulted in disruptive change for both users,

who must then create new login credentials, and for IT organizations, who must support the transition and resolve issues which may arise.

- Provide a means for an authorized user to regain access to a mobile device for which they have forgotten the password and, thereby, allowing the device to be used in the authentication system.

  The mobile phone has rapidly become a key component in many authentication systems due to its ubiquity, covering more than 2/3's of the world's population (GSMA Intelligence, 2017), and its ability to provide multi-factor capabilities through biometrics. With this rise in importance also comes a rise in the need to be able to securely recover from a lost password to unlock the device.

The research described here proposes a solution framework which addresses these requirements through a set of patents which advance the field. Taken together, these inventions provide a set of capabilities which help to increase trust and reduce fraud. These mechanisms are depicted as part of a larger whole in the system context diagram presented in Figure 1.

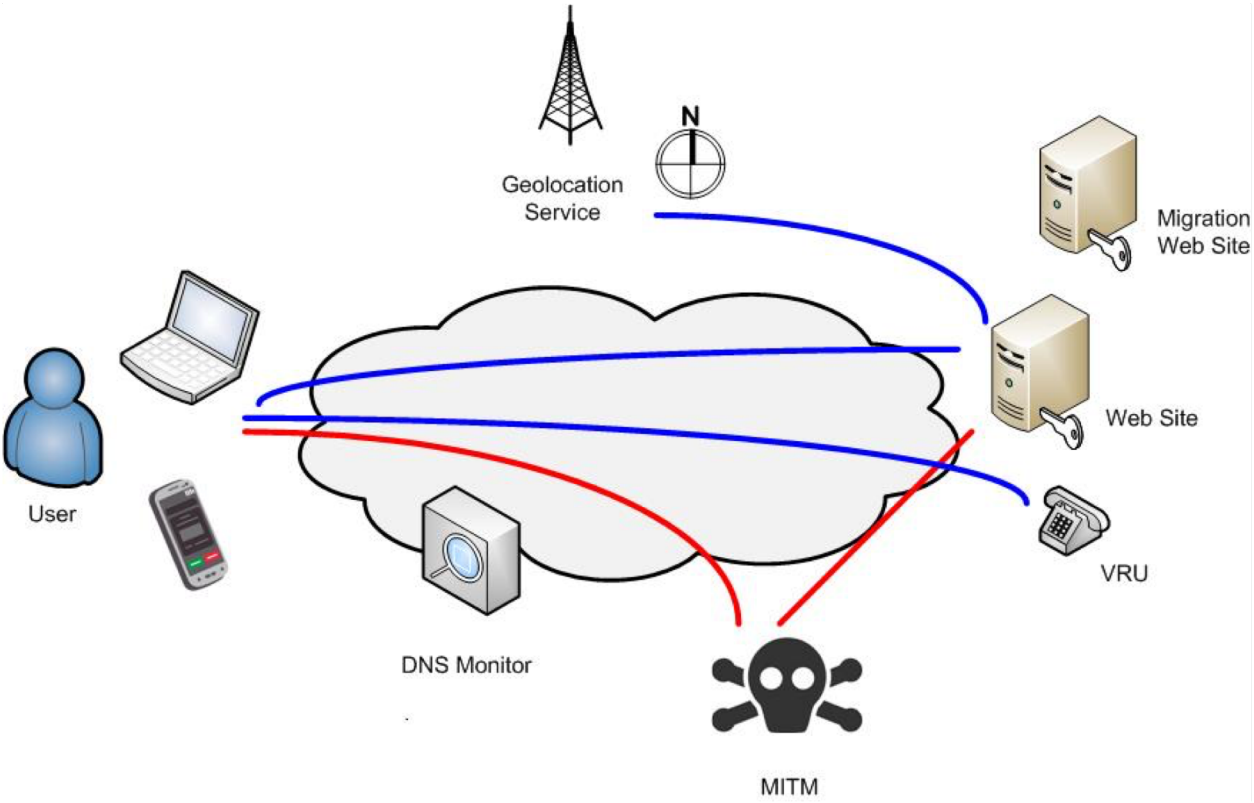


FIGURE 2: AUTHENTICATION SOLUTION SYSTEM CONTEXT DIAGRAM

The primary components of this solution along with a brief description of the authentication solution capabilities of each are as follows:

- **Web site authentication system –** This component verifies that the end user is who they claim to be. It accepts as input a set of credentials and authenticators. It also collects the IP address of the end user for use in geolocation.

- **Web site Voice Response Unit (VRU) –** This component performs the following tasks:
    - Answers calls from the end user
    - Verifies that calls are coming from the preregistered number for that user
    - Reads transaction details to the end user and solicits confirmation
    - Reads location details to the end user and solicits confirmation
    - Communicates confirmation (or denial) status to the web site authentication system
- **End user workstation –** This component contains a standard web browser capable of SSL/TLS encryption and certification verification.
- **End user mobile phone -** The end user's mobile phone will be configured to contain:
    - The phone number for the web site VRU stored in the contacts list
    - A transaction verifier app for decoding and displaying QR codes
    - A recovery app which allows for a trusted user to assist the end user in resetting their passcode in the case where this information has been forgotten
- **Geolocation service –** When provided with an IP address and mobile phone number from the web site authentication system, this component:
    - determines the geolocation associated with the IP address based upon ISP information lookup
    - determines the geolocation associated with the mobile device based upon communications service tower triangulation, GPS and other methods available to the mobile provider
    - confirms (or denies) whether these two locations are within an acceptable distance of each other as specified by the web site authentication service
- **DNS monitor –** This component monitors the network and alerts when incorrect DNS resolutions are provided based upon a table of known mappings
- **Migration web site authentication system –** This component provides a means to move users from one authentication system to another nondisruptively

2.1 Augmenting Existing Defenses

The patents and publications discussed here represent additional defenses intended to support the authentication process. These contributions were developed by the author in an effort advance the state of the art with a particular focus on detecting and defeating MITM attacks, which have proven to be extremely complex and difficult to overcome. The result of applying this work can create greater awareness of the threats to this key enabler of online transactions as well as greater confidence in the authenticity of the various parties to a transaction by thwarting a number of MITM and other impersonation attacks.

One way to lessen the risk of an MITM or other imposter attack is to use an out of band (OOB) communication path for some or all of the authentication activity. This way if an attacker has compromised the primary communication path, as might be the case through a phishing attack which has misdirected the user to an imposter site, the MITM would not be able to impersonate the user since the user's authentication data would not flow through the MITM site.

While most authentication technologies tend to focus on verifying the identity of the user, fewer tend to focus on enabling the user to verify the authenticity of the web site they are connected to. Typically, an encrypted SSL/TLS session is established between the user's browser and the web site. The browser validates the web site's digital certificate through a system of well-known trusted third-party certificate authorities. If verification fails, a warning message is displayed to the user letting them know that they could be dealing with an imposter. As previously

described, the problem with this is that most users simply ignore messages of this sort and proceed anyway so additional mechanisms are needed.

Therefore, there is a need to provide better mechanisms for ensuring that both parties to the transaction are, in fact, who they claim to be.

2.1.1 Geolocation as a Defense

Since most MITM attackers will not be physically near their victims, this discrepancy in distance would be a clue that an attack was underway.

Mobile Phone IP Address Location Correlation Service on page 16 provides a method for detecting an MITM. This is accomplished by comparing the geolocation of the user's mobile phone versus the location of the IP address associated with the user's session with the web site. In the case of an MITM, the web site would see the IP address of the MITM and realize that it was not physically near the location of the user's mobile phone and authentication would be denied. This invention also offers a degree of privacy protection for the user as outlined in the description of this patent subsequently in this document.

Detecting Man-in-the-Middle Attacks using Geolocation and Voice Response Telephony Prompts on page 17 leverages an OOB communication where the user calls into a predetermined VRU which tells them the approximate location that the legitimate web site believes the user's session with the site is emanating from. If this stated location is not physically near the user, then an MITM would be suspected and the user would abort the session.

Geolocation can also be used to improve the confidence that a user is who they claim to be as part of the authentication process.

Access Control Based Upon Expected User Location on page 19 goes beyond simple, country-based geographic restrictions such as "this user lives in country X so an attempt to login to their account from country Y should be disallowed." Such a system produces false rejections when the user travels internationally as well as false acceptances when the user is abroad, and an imposter attempts to login from the user's home country. This invention permits or denies access based upon where the user is expected to be at that particular moment based upon travel itineraries, work schedules and the like, thereby reducing the likelihood of both false rejections and false acceptances.

2.1.2 Authenticating Transactions

Reaching further past the basic authentication of the user would be the ability to authenticate details of the transaction the user is requesting.

Verification of Transactional Integrity on page 24 and Verifying Online Transaction Integrity and Authentication with QR Codes on page 26 provide mechanisms for a user to leverage an OOB channel for verifying details of the transaction they have requested. The former involves a call to a VRU, which reads details of the transaction to the user allowing them to confirm and proceed with the transaction or abort if the details do not match their intentions, indicating the presence of some form of tampering. The latter leverages a QR code generated by the web site containing the details of the transaction which is then read by an app on the user's mobile phone. This app then decodes the QR code and asks the user to confirm and proceed or abort the transaction if it appears that tampering has occurred.

2.2 Enabling Approaches Supporting the Authentication System

Detecting and Defending Against Man-in-the-Middle Attacks on page 31 provides a mechanism for detecting the presence of an MITM by observing a sudden increase in the number of authentication requests emanating from a single IP address. The assumption being that most users login at somewhat random intervals from a wide range of devices and locations. However, if a significant number of users start logging in from the same IP address to a degree not previously seen, then this could be an indication that these users have be redirected through an MITM, therefore, authentication should be denied.

Yet another way for an attacker to subvert the authenticity of the communications path would be to hijack the Domain Name System (DNS), which provides translation from human-recognizable names (e.g. www.ibm.com) into IP addresses (e.g. 9.1.2.3). Since users rarely remember the latter, the former makes for a more convenient way to indicate which site a browser should communicate with. However, if the DNS translator were to be under the control of an attacker, the attacker would be able to misdirect communications to an imposter site and have access to sensitive user information such as login credentials.

[Note: US patents 8,533,821 and 8,522,349 were split into separate patents by IBM attorneys in order to maximize legal protection and business value through the US Patent and Trademark Office. However, these are treated as one work for the purposes of this discussion.]

A System for Detecting the Presence of Rogue Domain Name Service Providers through Passive Monitoring on page 32 describes an invention which detects unauthorized DNS providers on a network by observing DNS traffic and comparing it to a list of known DNS mappings. If an incorrect resolution is supplied on the network, an alert is generated. As mentioned previously, (Wagner & Bryner, 2001) describe a scenario in which the ARP system is subverted. In fact, this invention could be applied to that protocol as well.

In some cases, an organization may need to migrate users from an existing authentication system to a new system. Doing this in a manner that is nondisruptive both to the users and to the support staff, which will be called upon to deal with issues that may occur, is challenging. Further, it may be required that password expiry intervals be preserved across the migration process so that users with newer passwords aren't required to change these again and users with older ones aren't given an artificial extension.

Migration Across Authentication Systems on page 35 describes a system where users can be migrated in controlled batches and, within these batches, spread out over to occur at the user's next login. The user's password is preserved as well as the password expiry interval maintained to ensure no violations of security policy.

Mobile phones are an increasingly important part of the authentication ecosystem. Since these devices are so common with nearly everyone using an IT system having at least one that is uniquely theirs, they have become a convenient way to satisfy the "something you have" criteria for authentication. Further, since many also provide a built-in biometric reader for a fingerprint or facial recognition, they can also satisfy the "something you are" criteria as well.

Given the critical role these devices play, the ability to regain access in a secure manner if the passcode to the device has been forgotten is of paramount importance since the inability to do so locks out a user not only from their device, but also from all the related services for which the mobile phone is relied on as an authenticator.

Mobile Device Password Reset on page 37 describes an invention which allows an authorized user to recover full access to their mobile phone through a series of interactions with a predetermined trusted user's device.

2.3 Integrative Use Cases

The following use cases demonstrate how this body of work could be used in combination to strengthen the authentication system with a particular focus on detecting and defeating MITM attacks. The details of the patents referenced in this section are described later in this document. The intent here is to show how these work together to provide a more holistic defense.

2.3.1 Web Customer Use Case

In this use case (depicted in Figure 3: Web customer Use Case), a banking customer wishes to transfer $1,000 from their savings account to their checking account using the web browser on their laptop. The customer is traveling abroad and opts to use the Wi-Fi service provided by his hotel. The customer also has a mobile phone which has been registered in advance with the bank.

1. In order to ensure that the public Wi-Fi network has not been compromised by a rogue DNS resolver, (Crume, 2017) is deployed on the network to spot suspicious activity.
2. The customer initiates a login to the bank's web site (2a). The bank sends an OTP to the customer (2b). The customer then calls the bank's VRU, who's number has been stored previously in the contacts list on his mobile phone, and enters the OTP (2c). When the VRU responds that the OTP is correct, the customer knows that he is on the correct web site rather than an imposter (2d). (Bravo & Crume, 2014)
3. Having previously received the customer's travel itinerary from a third-party booking web site, the bank knows that the customer should be in Brazil, rather than his home country, USA (3a). The bank verifies that the IP address the customer's session is originating from is, indeed, in Brazil, so the transaction can continue. (Note: If the address had been in the USA, where the customer would typically, the bank would actually need to reject the transaction because it knows the user is not actually there.) (Bravo & Crume, 2018) (3b)
4. While the customer is still on the phone, the VRU tells the customer that the system believes he is currently in Brazil. The customer indicates agreement and the transaction continues. (Bravo & Crume, 2014)
5. The customer then ends the call and proceeds to enter the details of their transaction (e.g. accounts, amounts, etc.). The bank then displays a QR code containing an encoded playback of these details which the customer then verifies with the bank's app running on his mobile phone. Confirming that the details are correct, the customer indicates consent to proceed with the transaction. (Bravo & Crume, 2017)

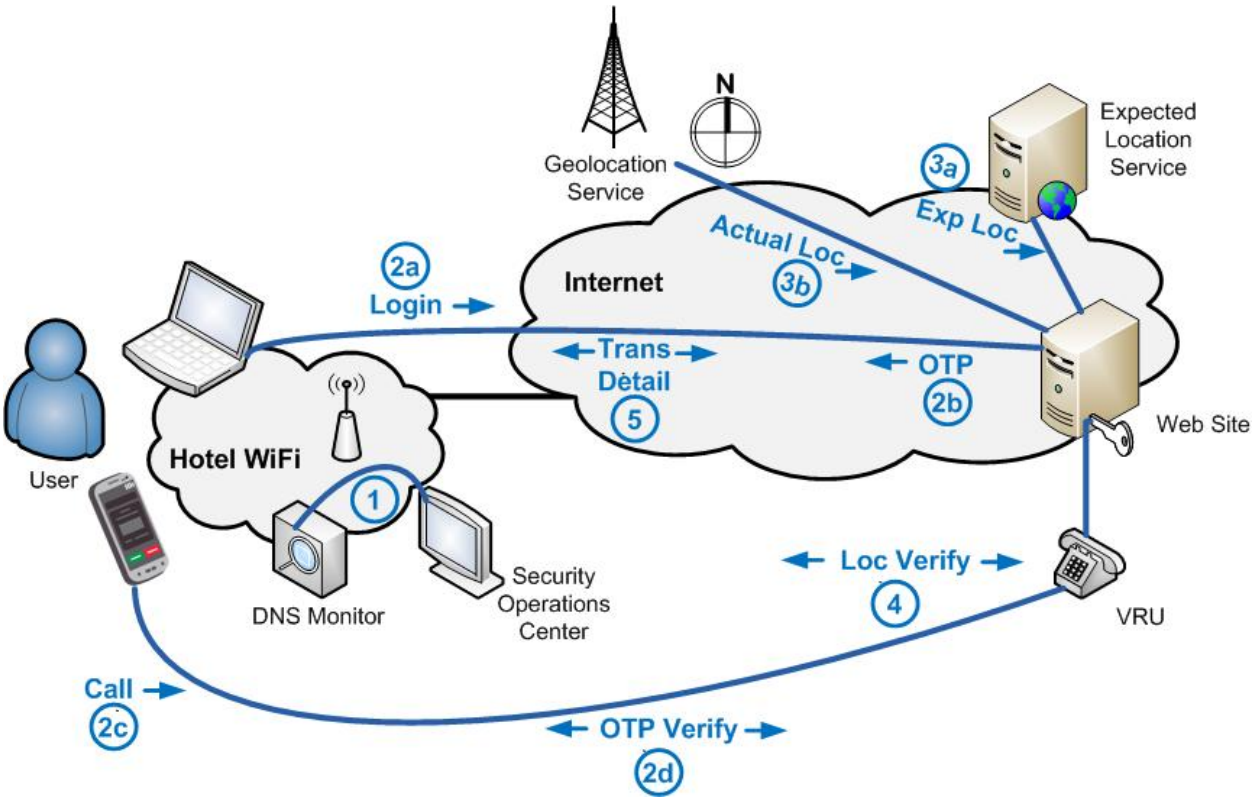


FIGURE 3: WEB CUSTOMER USE CASE

2.3.2 Mobile Device Use Case

In this use case (depicted in Figure 4: Mobile Device Use Case), the customer uses their mobile phone to conduct the banking transaction and leverages a different set of protection mechanisms.

1. The customer realizes they have forgotten the passcode to unlock their mobile phone. They use a landline phone in their hotel room to call a friend who has been previously registered as a trusted user to initiate the reset process. Through a series of communications between these individual's mobile devices, the phone is unlocked, and the customer regains full access to their phone and initiates login. (Bravo, et al., 2015)
2. The customer then logs in to the bank's web site using their mobile phone.
3. The bank sends the user's IP address and mobile phone number to a third-party location correlation service which verifies that the geolocation associated with each is within an acceptable distance so as to conclude that a MITM attack is unlikely. This follows from the fact that the IP address seen by the bank would have been that of the MITM, who would not likely be physically near the location of the customer's phone. (Bravo & Crume, 2014)
4. The customer then enters the transaction details on the bank's web site and is instructed to call the bank's VRU using the number they have previously stored in their contacts list. (4a) The VRU then reads the transaction details to the customer who then confirms that they are correct and the transaction proceeds. (4b) (Bravo & Crume, 2014)

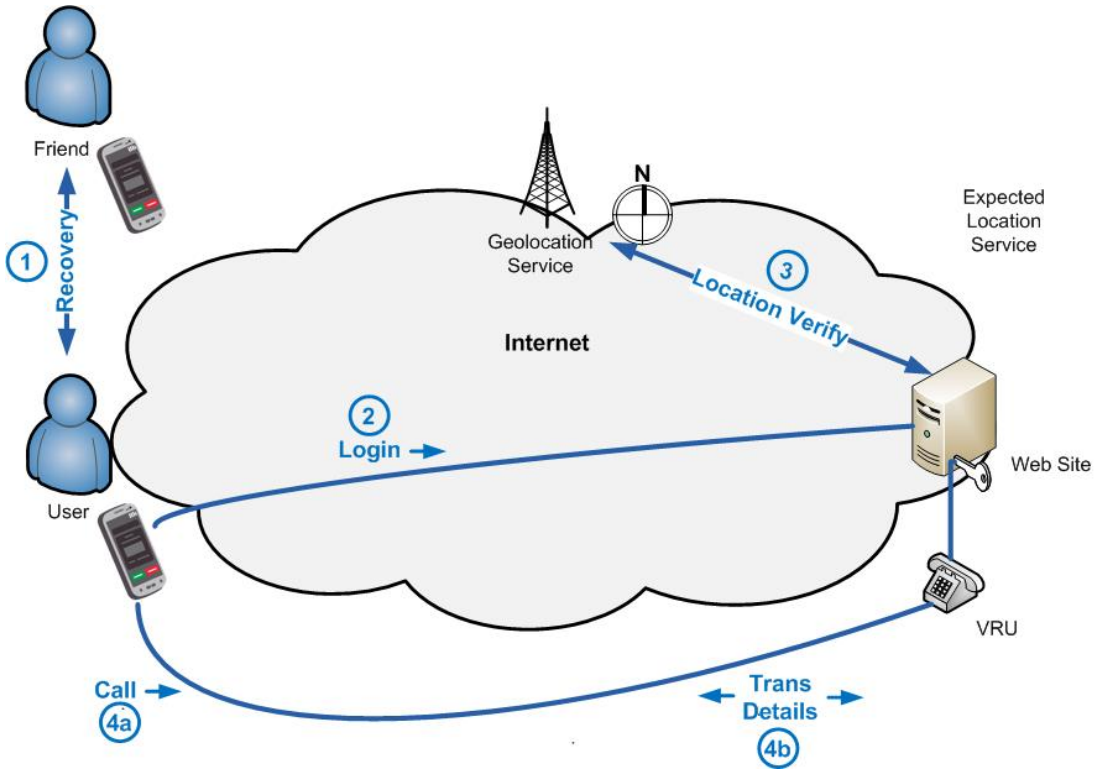


FIGURE 4: MOBILE DEVICE USE CASE

2.3.3 MITM Detection and Remediation

This use case highlights how the bank might determine the existence of a MITM attack affecting its customers and act to remediate by migrating these users to a new system which supports a more sophisticated access control system (e.g. risk-based access).

1. As depicted in steps 1 through 4 in the diagram below, the bank detects a significant number of login attempts from a wide range of customers all originating from the same IP address, which, notably, none have used before. The bank responds by blocking login attempts from this IP address until an investigation can be conducted. (Crume, 2013)
2. The bank concludes that a more effective access control system which authorizes requests based upon a risk score determined by a wide range of inputs would better guard against fraud. The decision is made to migrate customers in a phased, nondisruptive manner to the new system in such a way as to preserve existing login credentials as well as password expiry intervals. (Crume, 2010)

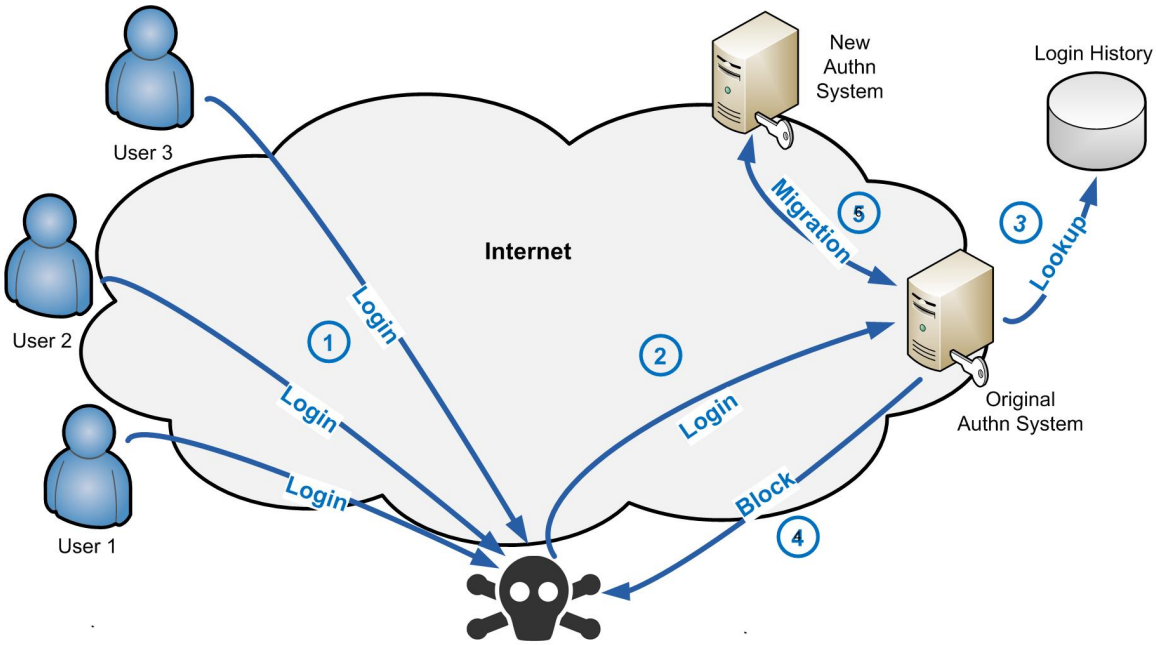


FIGURE 5: MITM DETECTION AND AUTHENTICATION SYSTEM MIGRATION

3 New Approaches to User-centric Authentication

The patents in this section focus on providing better assurance that the endpoints involved in a transaction are, indeed, who they claim to be.

3.1 Background and Related Works

In a phishing attack an end user is tricked into providing login credentials and/or other sensitive information by an attacker impersonating a legitimate web site. The reason this attack succeeds is that the victim is unable to adequately determine whether the web site in question is authentic. Most existing defenses require the end user to discern legitimacy based upon:

- the overall appearance of the site, which is easily faked,
- a specially-chosen site authentication image, which can be replicated in a man-in-the-middle attack, or
- the verification of the site's digital certificate, whose absence is often overlooked by the user. (Sunshine, et al., 2009)

Further, since the Internet is largely insensitive to geographical limitations due to its high degree of connectedness, attackers need not be limited to targets that are located physically near them. The removal of this limitation enables attacks to originate from any location and affect users on the other side of the world. This is an advantage attackers frequently leverage.

However, this also means that the likelihood that an MITM and their intended victim would be geographically near each other is small. In most cases, the attacker simply does not need to know or care about where their victim actually is. This lack of location awareness can, therefore, be exploited to work against the attacker.

In an attempt to mitigate risk, it has become more common for authentication systems to verify that a login is occurring from a legitimate geography in addition to verifying that those credentials are correct. This way a login from a country in which the organization does not do business might be rejected even if the user enters the correct userid and password. The assumption being that these credentials may have been stolen.

However, simple, country-based geographic restrictions such as “this user lives in country X so an attempt to login to their account from country Y should be disallowed” can result in false rejections when the user travels internationally. Further still, false acceptances can result when the user actually is abroad, and an imposter attempts to login from the user’s home country.

(Denning & MacDoran, 1998) proposes a system for determining geolocation as part of the authentication service by requiring devices to send their coordinates via a specially designed message. (Jaros & R., 2010) describes a location-based authentication system which provides a temporal element within a cryptographically secured message. (Camaisa & Samuelsson, 2007) uses browser cookies, which limit applicability to using the same browser for each session and may raise privacy issues for some users. (Kiliccote, 2008), (Kiliccote, 2008) and (Stoll, et al., 2008) use images, which the user must store and present for authentication. This approach lacks the degree of portability that many users desire. (Adida, n.d.) deals with web authentication only with no out of band process and is limited to browsers with JavaScript support, which may be turned off by security-conscious users.

(Constable, 2008) describes a system which would receive location information as input but does not actually determine the location. (Niedermeyer, 2008) uses location as determined by an unspecified location sensing device but does not compare this with the location as determined by the IP address of the user's browser. (O'Neil, 2002) does not leverage mobile phones and requires a special, localized network where all transactions are performed rather than a general purpose, public network. (Turnbull & Gedge, 2006) only applies to a restricted, previously designated workspace. (Clough, 2007) requires the addition of new data flows to the mobile phone backbone network as well as changes to message formats.

(Kato, 2013) leverages location data as part of the authentication process but is specifically designed for use with ATMs which have a known, fixed location and not with end users who may be mobile. (Wahl, 2010) relies specifically on calendar entries as the source for expected user location. (Goldberg & Boaz, 2013) relies on past logins to predict where a user might log in next. It also considers the distance between the current login location and the previous one to determine if the user could, in fact, have traveled that distance in the time that elapsed between the two.

(Kermode, 2009) and (Alicherry & Angelos, 2009) detect MITM attacks but do not leverage mobile phones and depend on the use of digital certificates. (Dewe, et al., 2009) requires a specialized app to be downloaded to the mobile device in order to perform cryptographic functions.

3.2 Enabling Approaches for User-centric Authentication

Patents described in this section extend and refine this defense by including additional aspects of location and leverage other mechanisms for determining coordinates.

3.2.1 Web Site Authentication

Much of the typical focus of authentication efforts has been on offering a service provider the ability to determine the identity of the user of that service. Instead, US patent 8,762,724 (Bravo & Crume, 2014) provides the ability for an end user to know whether the service, specifically, a web site, is, indeed, the one they intended to be transacting with.

This is done via a One Time Password (OTP) that the legitimate web site presents and which the user then repeats over a side communications channel -- in this case, a call from a phone preregistered with the web site. The Voice Response Unit (VRU) number that the user calls has also been determined in advance and communicated to the user who should have stored it in their device's phone book for easy retrieval and to avoid calling a fake number. The OTP is then verified by the VRU to ensure that it matches the one generated by the web site.

A potential phishing attack is then defeated because the attacker would not know the appropriate OTP to present to the user and the VRU would inform the user that no OTP match occurred.

When combined with traditional user authentication methods, this invention can close the loop with a return path for mutual authentication.

3.2.2 Mobile Phone IP Address Location Correlation Service

US patent 8,683,609 (Bravo & Crume, 2014) improves the confidence that a user is who they claim to be by comparing the user's geolocation, as determined by their IP address, to their geolocation as determined by their mobile phone service provider. The later may use mobile phone tower triangulation, for instance, to make this determination.

The notion here is that an MITM attacker would likely have a different physical location than the victim as there is no reason that the two would need to be co-located in the first. Therefore, when the attacker impersonates a user by sending transactions to the service provider under the user's identity, their geolocation, as determined by IP address, would differ significantly from the geolocation of the user, as determined by their mobile phone provider based upon characteristics of the mobile network.

This invention works by having the web site send the following to a third-party location correlation service:

- IP address of the user session
- mobile phone number of the user (from Caller ID or preregistered)
- a differential radius corresponding to the degree of risk the web site is willing to accept

The correlation service calculates the geographical location of the mobile phone through GPS or mobile tower triangulation and compares this to the geolocation location associated with the IP address. The service then returns an indication as to whether the two locations are within the specified distance of each other.

Further still, this invention offers a degree of privacy protection if the geolocation service is provided by a different organization than the organization being impersonated in the attack. This way the third-party service, likely the user's mobile service provider, who already must know the location of the device in order to route calls, can give confidence to the web site without divulging unnecessary details by providing a simple confirmation or denial of location proximity between the phone and the IP address.

3.2.3 Detecting Man-in-the-Middle Attacks using Geolocation and Voice Response Telephony Prompts

US patent 8,917,826 (Bravo & Crume, 2014) extends the protections described in the previous section (3.2.2 Mobile Phone IP Address Location Correlation Service) by providing the user a means for detecting MITM attacks in electronic transactions – typically with a web site.

The mechanism for doing so involves having the web site receive a request from a user, provide the user with an OTP and instruct the user to call a predetermined number to complete the verification process. Once the user has called, the voice response unit (VRU) will instruct the user to enter the OTP.

If the OTP matches, then the VRU will speak to the user the approximate location where they are believed to be, based upon the geolocation of the IP address determined by the web site. If the user agrees that their physical location is correct (within a reasonable degree of variance), then they confirm the transaction and processing continues.

The notion is that if an MITM is involved, then the web site will detect an IP address that is likely to be distant from where the user actually is at that time and, therefore, exposing this information to the user will allow them to know that something is amiss, and the transaction should be aborted.

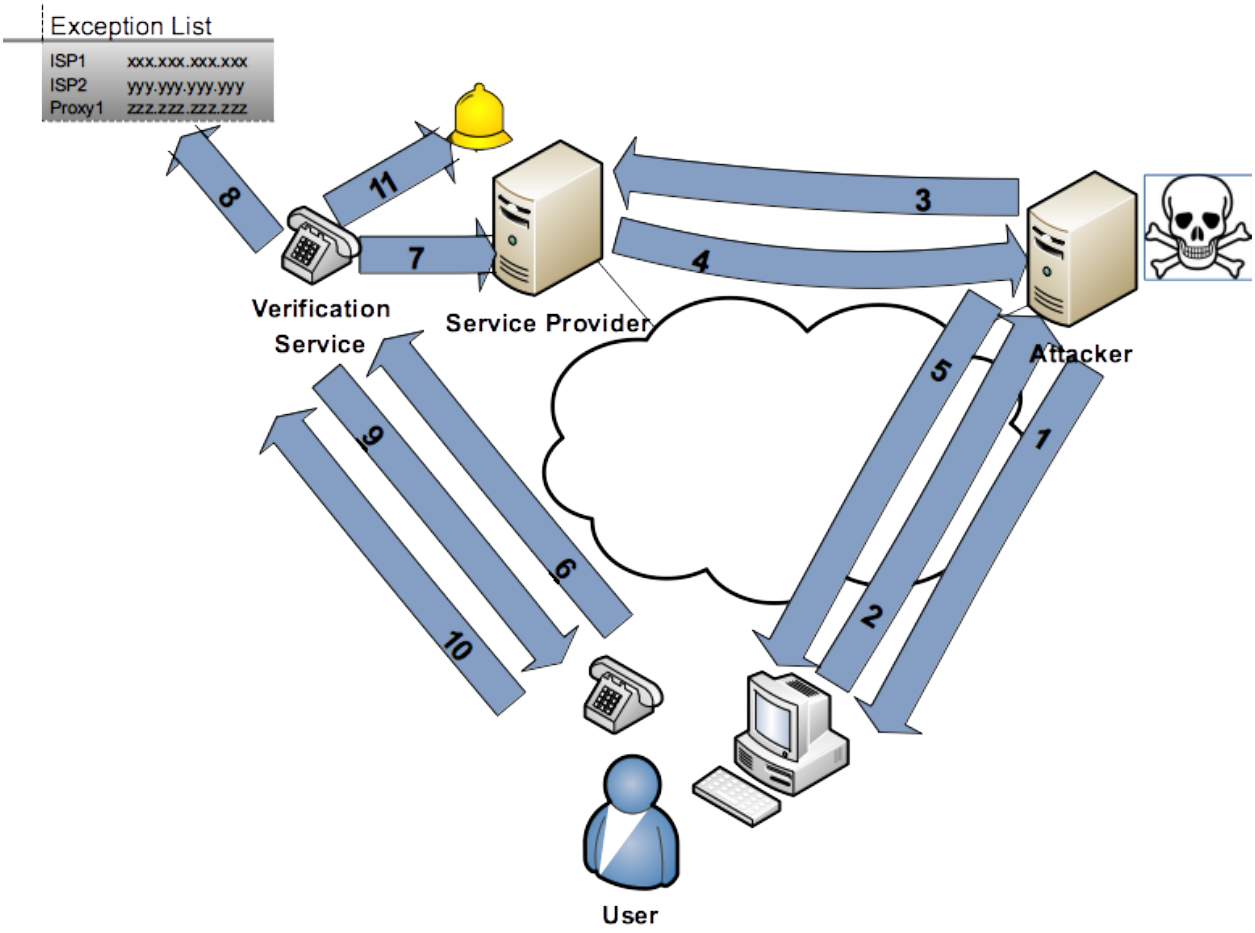


FIGURE 6: MITM DETECTION WITH GEOLOCATION AND VRU

1. Attacker lures User to initiate transaction. This could be the result of a phishing email, cross-site scripting attack or other.
2. User logs on to Attacker's system thinking it is the service provider and enters transaction details (e.g. transfer funds from savings account to checking)
3. Attacker starts a separate session with the service provider, logs in with User's credentials and enters modified transaction details (e.g. transfer funds from savings account to Attacker's account)
4. Service Provider generates OTP and sends (unknowingly) to Attacker along with instructions to call the Verification Service to verify details.
5. Attacker relays OTP and instructions to User
6. User places call to Verification Service via a predetermined phone number and enters OTP when prompted by VRU
7. Verification Center determines probable location of User based upon IP address of browser session (in this case the IP address points to Attacker)
8. If IP address is in the list of known exceptions no further verification is done
9. VRU asks User if their geographical location matches the one it has determined
10. Since Attacker's IP address is different from User's the VRU will state an incorrect location so User cancels transaction
11. Optionally, an alarm is sent to Service Provider for further investigation and analysis

3.2.4 Access Control Based Upon Expected User Location

US patent 10,027,770 (Bravo & Crume, 2018) extends beyond conventional IP address geolocation-based checking, which tends to be static and can result in false rejections in the case where legitimate users, who happen to be out of their normal area due to a business trip, vacation or temporary work assignment, are denied access.

In order to account for these exception cases and to provide a greater degree of accuracy and flexibility, which reduces false rejections and increases security, this invention takes as input, the user's *expected* location as determined by:

- travel itineraries,
- work schedules,
- vacation schedules and
- any other relevant data feeds.

For example, if the user's travel itinerary indicates that they should be in another country on a particular day and they try to login from that country, the system would allow this attempt. Conversely, a login attempt from the user's home country would be rejected if the user should, in fact, be visiting another country on that particular day. Neither of these use cases would be handled correctly by traditional IP address geolocation checking alone.

This invention creates a more adaptable authentication system which provides greater security and confidence based upon these trusted location data sources.

3.3 Impact of Contributions

The inventions described in this section build on and eliminate some of the limitations of the works cited previously in 3.1 Background and Related Works. By removing the need for browser cookies, predefined images, special networks and new protocols, this research describes mechanisms offering greater flexibility and security.

The current research extends the work of (Leung, n.d.), (Bychkov, 2007) and (Steinberg, 2007), which leverage OTP's as a means for detection, by adding location verification as well. US# 8,917,826 builds on concepts in US# 8,683,609 in that the user audibly hears where the system believes they are and the user – not the system – decides whether to continue with the transaction or not. US# 10,027,770 builds on (Wahl, 2010) by including other sources such as travel itineraries from a travel agent or provider, work schedules (e.g. for shift workers) and vacation schedules, thereby, providing a more generalized framework.

The inventions presented here have been the basis for subsequent research and inventions, as show in Tables 1-4. These consist of a total of 39 external citations from other companies such as Motorola, eBay, MasterCard, Microsoft, FedEx, Alibaba, Tata, Bank of America, Juniper Networks, Verizon, Xerox and Samsung. These references include patents from the US, UK, Japan, China, Singapore, South Korea and the World International Property Organization (WIPO). In addition, to these external citations, this work has been used by the inventors as the basis for further enhancements as demonstrated through 9 self-citations. In addition, these works resulted in 233 forward citations to yet other works.

(Note: US# 10,027,770 Expected Location-based Access Control was just recently granted a patent in July 2018 and has, therefore, not been in the public domain long enough to collect very many citations as of this writing.)

TABLE 1: CITATIONS FOR US# 8,762,724 WEBSITE AUTHENTICATION

Publication number	Assignee	Year	Forward Citations (38)	Title
External Citations (12)				
US10015153B1	EMC IP Holding Company LLC	2018	0	Security using velocity metrics identifying authentication performance for a set of devices
US8681965B1	Intervoice Limited Partnership	2014	1	Systems and methods for authenticating interactive voice response systems to callers
WO2011121566A1	Paytel Inc.	2011	14	A method for mutual authentication of a user and service provider
US9348992B2	eBay Inc.	2016	4	Linked identities
GB2488766A	Intercede Ltd	2012	9	Securely transferring data to a mobile device
US20130144620A1	Telcordia Technologies, Inc.	2013	1	Method, system and program for verifying the authenticity of a website using a reliable telecommunication channel and pre-login message
US20140359736A1	Deviceauthority, Inc.	2014	6	Dynamic voiceprint authentication
US20150082401A1	Motorola Solutions, Inc.	2015	1	Method and device for facilitating mutual authentication between a server and a user using haptic feedback
CN104954332A	腾讯科技（深圳）有限公司	2015	0	Website identification method and device
US9430630B2	Textpower, Inc.	2016	2	Credential-free identification and authentication
WO2017003379A1	Treebox Solutions Pte Ltd	2017	0	A method performed by at least one server configured to authenticate a user for a web service login
SG10201506058UA	Mastercard Asia Pacific Pte Ltd	2017	0	Method and system for website verification
Self-Citations (5)				
US10169759B2	IBM Corp	2019		Verifying online transaction integrity and authentication with QR codes
US8533821B2	IBM Corp	2013		Detecting and defending against man-in-the-middle attacks
US8683609B2	IBM Corp	2014		Mobile phone and IP address correlation service
US8838988B2	IBM Corp	2014		Verification of transactional integrity
US8917826B2	IBM Corp	2014		Detecting man-in-the-middle attacks in electronic transactions using prompts

TABLE 2: CITATIONS FOR US# 8,683,609 MOBILE PHONE AND IP ADDRESS LOCATION CORRELATION SERVICE

Publication number	Assignee	Year	Forward Citations (117)	Title
External Citations (15)				
US20130301595A1	Core Wireless Licensing S.A.R.L.	2013	6	Method of controlling a mobile terminal, and an associated mobile terminal
US20140282984A1	Microsoft Corporation	2014	1	Service relationship and communication management
US20160036777A1	Aaa Internet Publishing, Inc.	2016	1	Method of Near Real-Time Automated Global Geographical IP Address Discovery and Lookup by Executing Computer-Executable Instructions Stored on a Non-Transitory Computer-Readable Medium
US9648002B2	Microsoft Technology Licensing, Llc	2017	0	Location-based user disambiguation
US9087213B2	Fedex Corporate Services, Inc.	2015	9	Systems and methods for rule-driven management of sensor data across geographic areas and derived actions
JP5751060B2	ブラザー工業株式会社	2015	7	Printing apparatus and a printing system
CN102594908B	华为技术有限公司	2014	5	Method, equipment and system for transmitting network contents
KR101392047B1	주식회사 엘지씨엔에스	2014	6	User verification server and the mobile terminal of the user verification method, do this
JP5763592B2	株式会社野村総合研究所	2015	2	Authentication system and the authentication device
US9355231B2	Telesign Corporation	2016	41	Frictionless multi-factor authentication system and method
US9124582B2	Fmr Llc	2015	37	Mobile security fob
CN104580112B	阿里巴巴集团控股有限公司	2018	2	Kind of business authentication method, system and server
WO2015060950A1	Alibaba Group Holding Limited	2015	0	Method and system for authenticating service
CN105592074A	中国银联股份有限公司	2016	0	Method and system of mobile device cooperation authentication on the basis of geographic position
US20190037071A1	Tata Communications (America) Inc.	2019	0	Mobile roaming and authentication
Self-Citations (3)				
US10169759B2	IBM Corp	2019		Verifying online transaction integrity and authentication with QR codes
US8533821B2	IBM Corp	2013		Detecting and defending against man-in-the-middle attacks

US20100269162A1	IBM Corp	2010		Website authentication
US8838988B2	IBM Corp	2014		Verification of transactional integrity
US8917826B2	IBM Corp	2014		Detecting man-in-the-middle attacks in electronic transactions using prompts

TABLE 3: CITATIONS FOR US# 8,917,826 DETECTING MAN-IN-THE-MIDDLE ATTACKS USING GEOLOCATION AND VOICE RESPONSE TELEPHONY PROMPTS

Publication number	Assignee	Year	Forward Citations (77)	Title
External Citations (9)				
US9444812B1	Seven Networks, Llc	2016	38	Systems and methods for authenticating a service
JP5763592B2	株式会社野村総合研究所	2015	2	Authentication system and the authentication device
KR101451214B1	주식회사 엘지씨엔에스	2014	15	Payment method, server performing the same, storage media storing the same and system performing the same
US20150032620A1	Bank of America Corporation	2015	7	Communication network for collecting data and executing electronic transaction services
US9722801B2	Juniper Networks, Inc.	2017	6	Detecting and preventing man-in-the-middle attacks on an encrypted connection
US9515984B1	El Toro.Com, Llc	2016	3	Determining and utilizing one or more attributes of IP addresses
US9407762B2	Bank of America Corporation	2016	5	Providing enhanced user authentication functionalities
US10091193B2	Mastercard International Incorporated	2018	1	One time passcode
US10148816B2	Verizon Patent and Licensing Inc.	2018	0	Interactive voice response (IVR) call authentication
Self-Citations (1)				
US10169759B2	IBM Corp	2019		Verifying online transaction integrity and authentication with QR codes

TABLE 4: CITATIONS FOR US# 10,027,770 EXPECTED LOCATION-BASED ACCESS CONTROL

Publication number	Assignee	Year	Forward Citations (1)	Title
External Citations (3)				
US20160127873A1	Samsung Electronics Co., Ltd.	2016	0	Method of predicting location of rendezvous and electronic device for providing same

US9747768B1	Xerox Corporation	2017	1	System and method for proving physical presence
US20180145990A1	Microsoft Technology Licensing, Llc	2018	0	Multi-factor authentication using positioning data

4 TRANSACTION-CENTRIC AUTHENTICATION

The contributions in this section focus on providing greater assurance that the transaction details have not been altered by an attacker such as an MITM.

4.1 BACKGROUND AND RELATED WORKS

The increasing dependence upon online channels to conduct sensitive transactions such as Internet banking and e-commerce carries with it an increasing risk that these transactions could be subverted by a determined attacker. A rise in the prevalence of malware which can act as an MITM logging keystrokes, redirecting network traffic, eavesdropping, etc., creates a direct threat by increasing the likelihood that fraud may be committed remotely.

For instance, a computer could be infected by malware capable of subverting even strong, second factor authentication mechanisms. The user of such a compromised machine could be prompted by the malware to authorize a transaction of one sort while the MITM modifies the request before submitting it.

An example of this might be the case where a user requests that funds be transferred to another account, authenticates the transaction and then the MITM modifies the transaction to divert funds to a different account -- possibly changing the amount in the process as well. A special case of this type of attack involving a compromise of the user's browser is also known as a man-in-the-browser (MITB) attack and is being seen with increasing prevalence.

(Bravo & Covalla, 2006) shows how strong authentication can be accomplished inexpensively and conveniently by entering a 4-digit OTP via a pre-registered mobile phone. (Jones, et al., 2008) requires the user to call the service provider first to initiate the transaction using the mobile device for verification.

(Rados, et al., 2009) involves authenticating the user via an OTP generated by the mobile device. (Calabrese & Stemer, 2008) and (Law, et al., 2008) involve verifying transaction details through entering an OTP or PIN on the mobile device. However, this approach leaves a greater potential for MITM attack since the same channel is used for all communications.

4.2 ENABLING APPROACHES TO TRANSACTION-CENTRIC AUTHENTICATION

4.2.1 VERIFICATION OF TRANSACTIONAL INTEGRITY

Current systems typically rely solely on memorized passwords to authenticate a user, but these can be discovered and replayed. This invention builds on (Bravo & Covalla, 2006) where the user is required to send (via mobile phone messaging) an OTP chosen randomly by the server. The server then verifies that the OTP sent by the user matches the one it chose for that log in and that it was sent from the mobile phone number registered to that user.

US patent 8,838,988 (Bravo & Crume, 2014) adds protection against an MITM that might attempt to modify a transaction by providing data integrity checking and transaction-level authentication through an out of band communications channel -- specifically, a mobile phone call -- which the MITM attacker would not have access to.

This invention may optionally leverage special mobile phone carrier-based service messaging to initiate the call (i.e. a sequence typically beginning with # or * and followed by a few alphanumeric digits assigned to this service). As such, the risk of Caller ID spoofing is greatly reduced, thereby providing greater confidence that the caller is, in fact, the authorized user along with the additional benefit of not charging the user for air time for the call.

Once the user has called the predetermined number and entered the OTP supplied by the web site, the VRU will state audibly the details of the transaction (e.g. amounts, accounts, transaction type, etc.) and ask the user to confirm these details. If an MITM has tampered with the transaction (e.g. example changed the account that funds are to be transferred to), this will be obvious to the user, who can then indicate to the VRU that the transaction should be aborted.

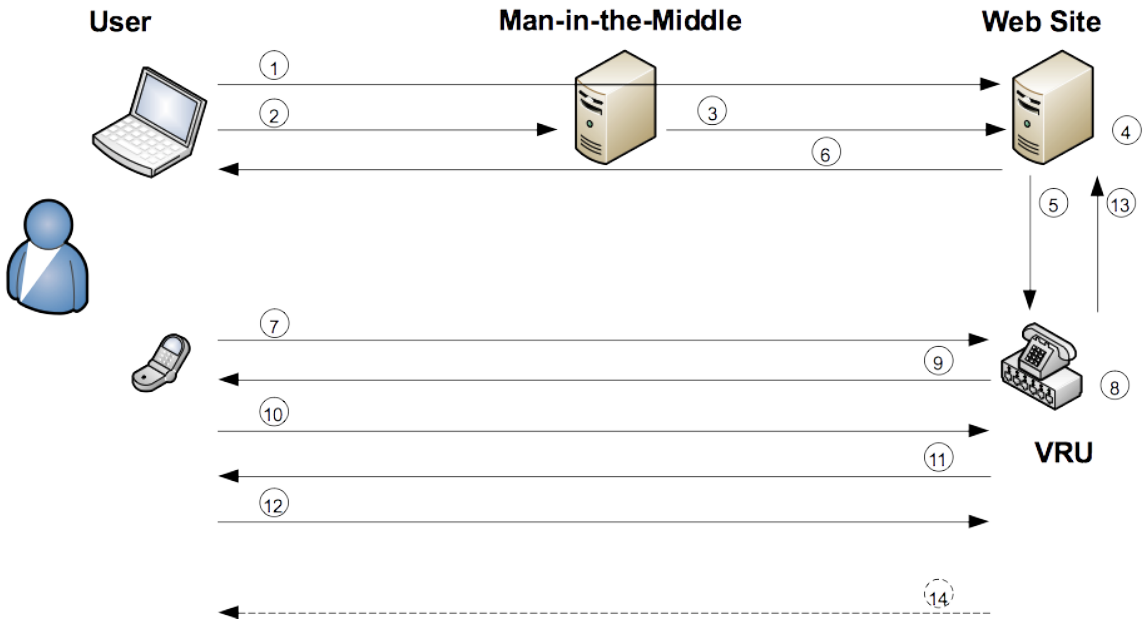


FIGURE 7: FLOW DIAGRAM FOR TRANSACTIONAL INTEGRITY CHECKING

The following describes the steps involved in a transaction exploiting this technique. (Note: it is assumed that the user's OS or browser has already been compromised by a MITM remote monitor.)

1. User logs into web site (e.g. a financial institution, e-commerce merchant or similar) passing through MITM
2. User initiates a transaction such as a transfer of funds or purchase order
3. MITM intercepts the transaction and modifies the details such as changing the destination account for the transfer or amount of goods purchased
4. Web site parses the transaction and generates a unique, time-sensitive OTP which serves as a transaction id
5. Web site sends the OTP and the characteristics of the call to the voice response unit (VRU) and instructs it to expect a call from the previously registered mobile phone for this user
6. Web site instructs the user to place a special service call using the predetermined mobile phone dialing sequence (e.g. "#mybank") and enter the OTP for this transaction
7. User places the call
8. Web site's VRU, which may, in fact, be run by the mobile phone carrier or other 3rd party, determines user's phone number
9. VRU asks user to enter OTP
10. User enter OTP from web site
11. VRU reads transaction details to user and instructs user to confirm transaction details by pressing 1 or reject by pressing 2 (or simply hanging up)
12. User realizes that transaction details do not match and presses 2
13. VRU informs web site about the acceptance or rejection of the transaction

14. Optionally user is asked whether they would like web site operators to follow up by investigating the source of the discrepancy

4.2.2 Verifying Online Transaction Integrity and Authentication with QR Codes

(Bravo & Crume, 2014) verifies the details of a transaction providing a mechanism to detect the presence of tampering. This invention (Bravo & Crume, 2017) uses a different mechanism to accomplish these ends by providing a means for allowing the user to verify transaction details on a mobile device, thereby exposing tampering by an MITM.

Encoded details are sent from the transaction server to the user in the form of a QR code displayed in the user's web browser. The user then scans this image with a purpose-built mobile app, which presents the decoded details and asks the user to confirm or abort the transaction. Since the mobile device will have been preregistered with the transaction server, the confirmation message also serves as an additional authentication factor thereby increasing confidence for both the user and the server that the transaction is legitimate.

The mobile app uses an out-of-band channel (i.e. the mobile phone network) to transmit confirmation, so any tampering with the transaction's details by an MITM can be detected during the confirmation step and the attack thwarted.

Further, since the mobile device is preregistered with the transaction server, the confirmation message from the verifier app will not only ensure transactional integrity but also provide an additional authentication factor.

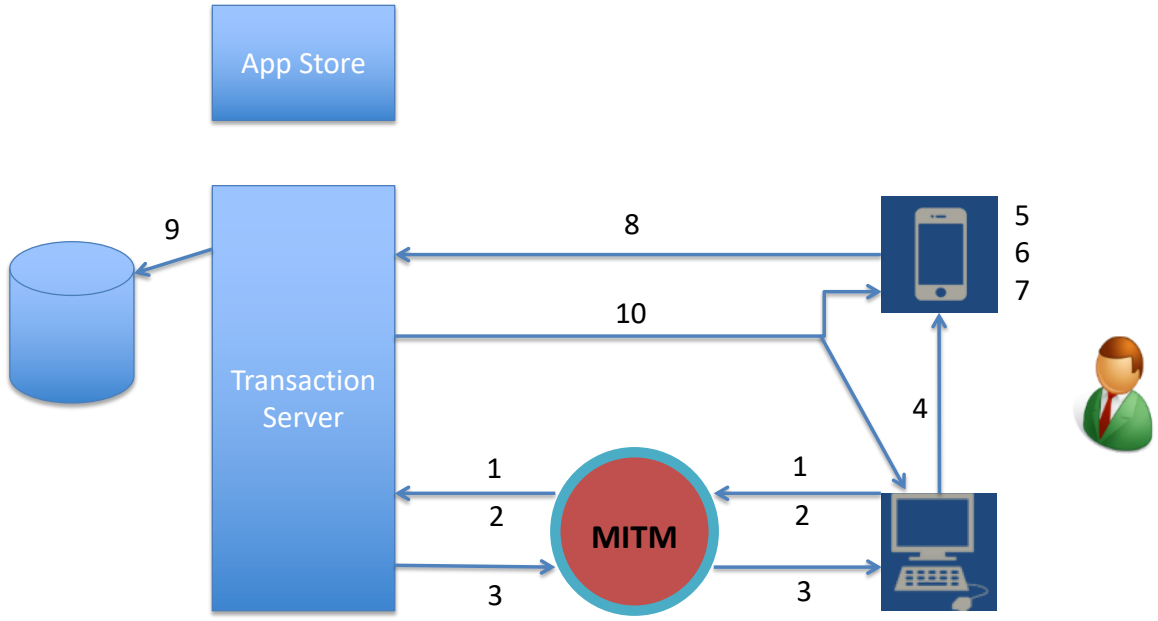


FIGURE 8: TRANSACTION INTEGRITY WITH QR CODES FLOW DIAGRAM

1. User logs into transaction server from computer browser with userid/pw (or another authentication method)
2. User creates a transaction using browser
3. Transaction server returns a QR code containing encoded transaction details to the user's browser where the image is displayed
4. User scans QR code with specialized verifier app on preregistered mobile device
5. Verifier app decodes transaction details
6. Verifier app displays details of transaction and asks user to confirm
7. User hits confirm button in verifier app if details are consistent with original request or abort button if not
8. Verifier app sends confirm or abort message to transaction server via mobile channel (i.e. SMS or data connection)
9. Transaction server verifies that message is from authorized user matching registered device/user in data base
10. Transaction server completes the transaction if details are confirmed or aborts if not and sends response

4.3 Impact of Contributions

The inventions described in this section build on the related works described in 4.1 Background and Related Works and reduce the likelihood of MITM attack by leveraging out of band communications channels. The first invention described in this section does essentially the reverse of (Jones, et al., 2008), where the transaction is initiated online (via web browser, ATM or mobile device) and a voice call is used to confirm the integrity of the transaction, thereby, closing the loop by offering an alternative path for verification. The second invention builds on (Rados, et al., 2009) by also verifying transaction details after authentication.

The inventions described in this section have been the basis for subsequent research and inventions, as show in Table 5. These consist of a total of 4 external citations from Bank of America and iSignthis. These references include patents from the US and Canada. In addition, to these external citations, this work has been used by the inventors as the basis for further enhancements as demonstrated through 5 self-citations. In addition, these external citations resulted in 16 forward citations to yet other works.

(Note: US# 10,169,759 Verification of Transactional Integrity and Authentication with QR Codes was just recently granted a patent early in 2019 and has, therefore, not been in the public domain long enough to collect any citations as of this writing.)

TABLE 5: CITATIONS FOR US# 8,838,988 VERIFICATION OF TRANSACTIONAL INTEGRITY

Publication Number	Assignee	Year	Forward Citations (16)	Title
External Citations (4)				
US9595035b2	Bank of America Corporation	2017	2	Service for Exceeding Account Thresholds Via Transaction Machine
US9595036b2	Bank of America Corporation	2017	13	Service for Exceeding Account Thresholds Via Mobile Device
US9508076b2	Bank of America Corporation	2016	1	Service for Account with Unavailable Funds or Credit Using a Passcode

CA2972104a1	Isignthis Ltd	2016	0	Securing A Transaction
Self-Citations (5)				
US10169759b2	IBM Corp	2019		Verifying Online Transaction Integrity and Authentication with QR Codes
US8533821b2	IBM Corp	2013		Detecting and Defending Against Man-In-The-Middle Attacks
US8683609b2	IBM Corp	2014		Mobile Phone and IP Address Correlation Service
US8917826b2	IBM Corp	2014		Detecting Man-In-The-Middle Attacks in Electronic Transactions Using Prompts
US20100269162a1	IBM Corp	2010		Website Authentication

5 AUTHENTICATION SYSTEM SUPPORT

Section 3 describes mechanisms which provide greater confidence that the parties to a transaction are, in fact, who they claim to be. Section 4 descries mechanisms which ensure that transaction details have not been tampered with. In addition, there is a need to further enhance the systems that support the authentication process. The contributions in this section broadly support this area by offering additional defenses and as well as capabilities which allow for nondisruptive migration to a new authentication system and a means for secure recovery of a mobile device for which the password has been lost.

5.1 BACKGROUND AND RELATED WORKS

Since an MITM attack can affect the ability to correctly authenticate a user, any improvement in MITM detection and defense can help support the authentication process.

As discussed previously, various mitigation techniques have been applied to defeating MITM attacks. While digital certificates could provide a reasonable measure of protection, they have primarily been limited to server-side deployments. This is due to the difficulty and expense of deploying and managing a vast number of certificates across a large end user population. Further complicating matters is the fact that those users may have limited technical skills and may also be highly mobile, using many different nodes to conduct transactions from. As a result, digital certificates tend only to provide one-way authentication (i.e. server proves identity to user) in the best of real-world circumstances. The fact that most users typically ignore warning messages of invalid server certificates means even this protection is often ineffective (Sunshine, et al., 2009). Digital certificates may also be used to subvert security if they are self-signed and the client and server fail to detect this condition. (Callegati, et al., 2009)

Another increasingly popular defense is to use "strong" authentication mechanisms such as security tokens, smart cards or biometrics to ensure that the end user is who they claim to be. The problem with these defenses is that in the MITM case the digitized authentication data is simply passed directly through the intermediate node making it unnecessary for the attacker to actually possess the token, smart card or physical characteristic being measured.

Still another technique for alerting end users that they are being lured into logging into a bogus web site involves the presentation of a graphical image preselected by the user. During login, if the user does not see the image they selected during registration, something which only they and the legitimate Web site should know to present, then they know to abort the authentication process. However, in an MITM case, the target Web site presents the image to the MITM node thinking it is the end user and the MITM node relays this image to the real end user making them believe that the attack node is legitimate, thereby rendering this defense ineffective.

Also, key to the integrity of the authentication process is the Domain Name Service (DNS), which resolves alphanumeric domain names (e.g. www.ibm.com) into numeric IP addresses (9.xxx.yyy.zzz). This service is provided by a loose collection of servers scattered around the Internet as well as within local Intranets. If, however, the information supplied through this service comes not from an authorized source, but rather, an attacker's system supplying incorrect information, network traffic could be impeded in a denial of service (DOS) attack or misrouted in a spoofing attack resulting in sensitive traffic being delivered to untrusted systems. (Conti, et al., 2016)

One way that these services could be subverted would be for an attacker to set up an "evil twin" Wi-Fi hot spot which impersonates a trusted wireless access point and establishes itself as an MITM, which can examine and modify

all traffic coming into and going out of the rogue network. Another way would be for the attacker to set up a rogue server which hijacks network services by broadcasting to all nodes in the network that it is online and available to process requests. This is due to the fact that in many cases the last server to broadcast will be considered authoritative by other nodes in the network. (Callegati, et al., 2009) shows how ARP and DNS poisoning attacks can be carried out in this manner. (Belenguer & Calafate, 2007) describe available tools which can carry out such ARP poisoning attacks.

Another area where significant challenges can be encountered is when there is a need to migrate users from one authentication system to another. Typically, users are required to either change their password or re-register as credentials are not transferable. In addition, there may be a desire to provide a phased transfer where the number of users to be migrated at any one point in time is controlled in case problems are encountered with the new system. Finally, it may be desired that current password expirations be maintained across the migration process so as not to violate security policy by resetting these intervals on the new system while simultaneously not upsetting users by making them choose new credentials.

Finally, current methods for resetting lost/forgotten mobile phone passwords require the user to perform a “master reset" on the device. Unfortunately, this action typically erases all settings including contacts, applications and other personalization data. Alternatively, a master reset may be automatically triggered after a predetermined number of failed attempts to enter the password. In neither case will the user be able to recover data on the device unless they have backed up the device to a cloud storage service or local computer. Even with such a backup, the restoration process can be time-consuming and may not bring back all the data and put the phone back in its original state, especially if the device was customized significantly.

Since mobile phones are increasingly being used as security tokens and biometric readers, they have become an indispensable part of the authentication ecosystem. The inability to unlock this device could not only deny the user access to all the data they have on the phone, but also, the ability to access other services which leverage the phone as an authenticator.

(Fremberg, 2005) requires that the client system be loaded with software, which will communicate with the server to authenticate. This requirement is often impossible to enforce as user end points are not under the control of the service provider in many scenarios. (Crilly Jr., 2005) deals with wireless networking “interlopers” and depends upon the ability to detect anomalies in the signal based upon intrusion activities. In the case of phishing and general purpose MITM attacks, no such assumptions can be made with regards to the underlying networking environment since they traverse the global Internet. (Lee & Choi, n.d.) provides a mechanism for detecting an MITM that is dropping packets but requires that all nodes in the path participate in the scheme, which would be an unreasonable requirement in a consumer-based MITM defense.

DNS Watcher (SB-Software, 2005) is a service which performs a DNS health check by polling known DNS servers. (Doyle, et al., 2006), (Chesire, 2006), (Olson & Ogorek, 2009) and (Shaobu, 2011) also employ similar polling mechanisms.

(Gillet & Mantyla, 2011) resets a mobile phone password by communicating with a trusted contact, who then sends a password to the device in order to unlock it. (Hadizad, 2014) uses a similar process as the previous invention but the new password is communicated acoustically instead.

5.2 Enabling Approaches Supporting the Authentication System

5.2.1 Detecting and Defending Against Man-in-the-Middle Attacks

MITM attacks share a detectable characteristic which can be used to predict to some reasonable certainty that impersonation is taking place. Once detected, the legitimate web site can send a message which will be relayed by the MITM node to the user informing them (as well as alerting web site support staff) of the potential vulnerability and ending the session.

This observable characteristic, which is shared by successful MITM attacks, is that:

> *"to the target web site, it appears that a large number of different end users are simultaneously logging on from the same IP address -- the address of the MITM proxy."*

Of course, this behavior alone would not always indicate malicious activity, but if the timing were such that certain definable thresholds were exceeded from a single, previously unknown address within a specific interval of time, then further investigation or even automated defenses would be warranted.

US patents 8,533,821 (Crume, 2013) and 8,522,349 (Crume, 2013) add a mechanism as a side process to the authentication system which checks login details (e.g. IP address, userid) to see if a significant number of users have simultaneously started logging in from the same IP address within a given time window. If this threshold is exceeded, then an alert can be generated and, optionally, the login attempt denied.

Specifically, the target Web site (e.g. a legitimate bank) would install an MITM detection and response component which would:

- determine the origination of incoming login requests
- check those requests against a blacklist of previously suspected MITM nodes
- check to see if the MITM detection threshold had been exceeded
- deny the login request if either of the previous conditions are violated or
- allow normal login to proceed if thresholds have not been exceeded

The thresholds would be customizable by the target organization according to their tolerance for risk (much like a biometric system or intrusion detection system must be tuned to minimize false positives while not overlooking real attacks). These observed values and associated thresholds could be expressed as follows:

- N = number of userids logging in from the given IP addr
- Nt = threshold of acceptable number of userids logging in from any given IP addr
- T = time interval over which logins from a given IP addr have been attempted
- Tt = time interval threshold triggering suspicion

This data would be processed as follows:

```
If N>Nt and T>Tt then
        suspect MITM attack
otherwise
        proceed with login and record details
```

A table is maintained which keeps track of the various userids which have logged in from a given IP address. One possible implementation would involve a hash tree which indexes the IP addresses and then points to a linked list of userids which have logged on from that address, however, other options exist.

Some advantages to this technique are that:

- the threshold can be tuned to suit the risk tolerance of the target organization
- detection can be automated
- countermeasures can be automated to limit further damage
- automated detection and response allow for constant vigilance by providing a continuous, 24x7 defense
- the basic technique can be extended beyond web spoofing/phishing attacks to other types of MITM scenarios
- the more "successful" the attacker is at luring victims, the more likely the attack will be detected and repelled

In order to improve efficiency, this invention also maintains a whitelist of known, legitimate proxies that users' sessions might be routed through so as to avoid false alarms.

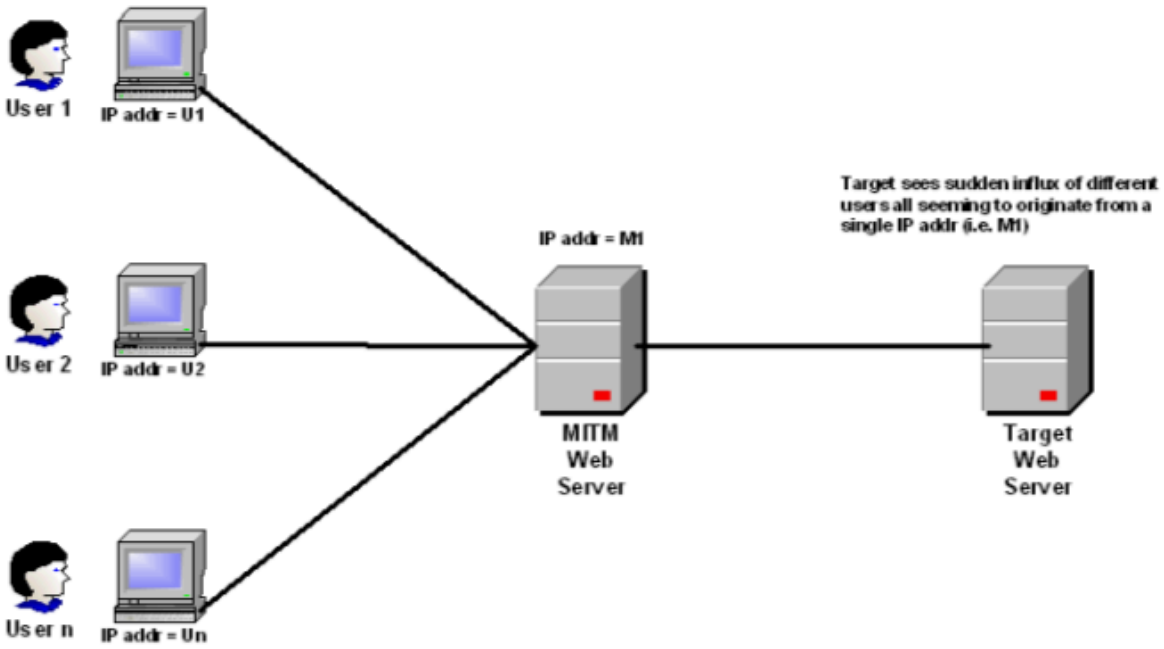


FIGURE 9: MITM COMPROMISING MULTIPLE USERS

[Note: US patents 8,533,821 (Crume, 2013) and 8,522,349 (Crume, 2013) were split into separate patents by IBM attorneys in order to maximize legal protection and business value through the US Patent and Trademark Office. However, these are treated as one work for the purposes of this discussion.]

5.2.2 A System for Detecting the Presence of Rogue Domain Name Service Providers through Passive Monitoring

An attacker could impact the integrity of an authentication system by rerouting traffic to an imposter web site. One way this could be accomplished would be to insert a rogue DNS provider which misroutes traffic to the attacker's web site rather than the legitimate one intended by the user.

This invention described in US patents 9,648,033 and US# 9,225,731 (also registered as German patent 102013208923) create a system for detecting the presence of rogue DNS protocol servers through the use of a passive monitor which looks for spoofed traffic of this sort. The monitor is positioned at a strategic point in the network such that it is able to observe traffic flows from other nodes. When the monitor detects DNS resolutions that don't match those from a preconfigured list of known DNS entries, it sends an alert with details of the suspicious activity.

This invention could be implemented either as a software tool running on as a general-purpose computer with access to network traffic, as a feature of an intrusion detection or intrusion prevention system (IDS/IPS) or as a stand-alone network appliance.

A Known DNS Resolution table is preconfigured, which contains a list of domain name to IP address mappings that are known to be valid. These mappings could also be expressed using wildcards or ranges of addresses in order to handle more or less specificity. (Note: This list need not be comprehensive to be of value. As a matter of practicality, it is likely that only a selected few well-known, sensitive hosts will be configured to serve as a representative sample.)

As mentioned previously, (Wagner & Bryner, 2001) describe a scenario in which the ARP system is subverted. In fact, this invention could be applied to that protocol as well.

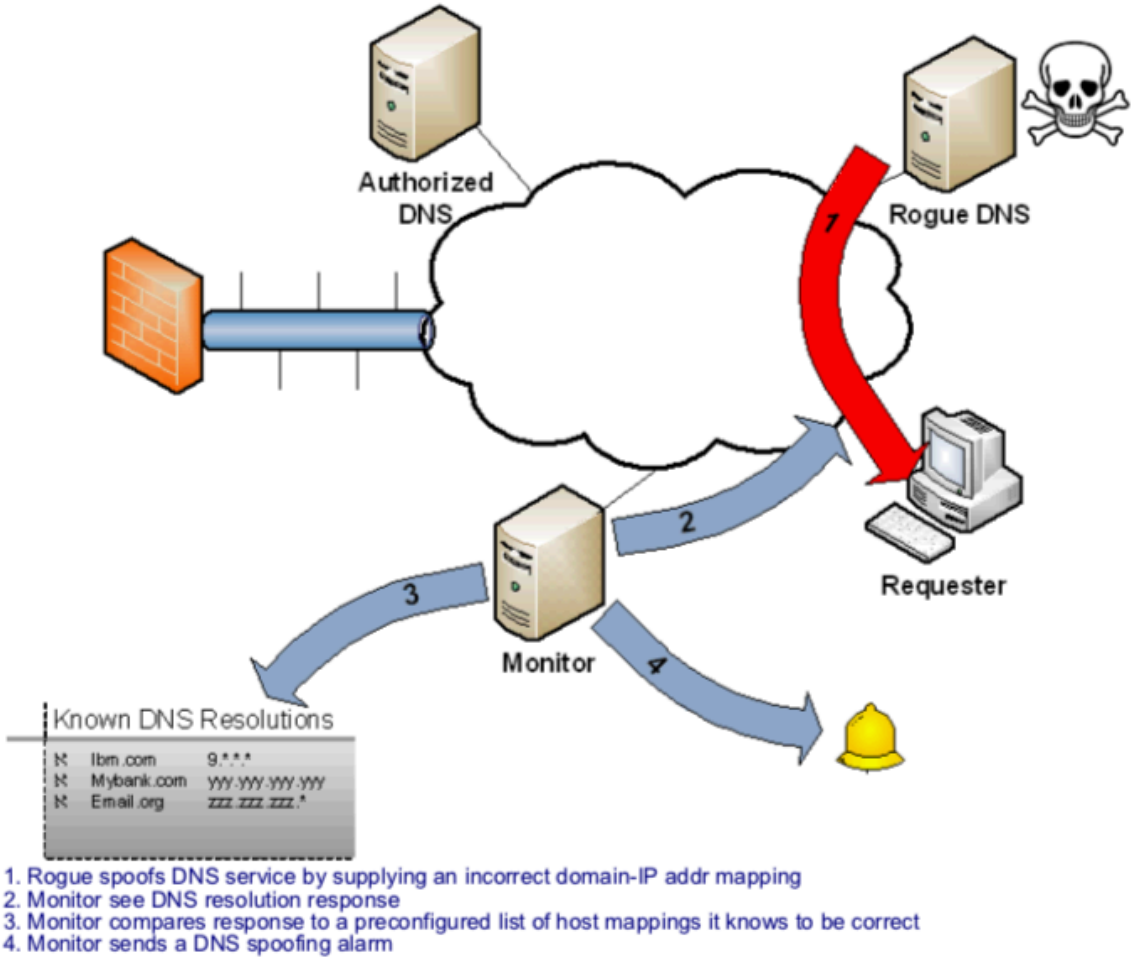


FIGURE 10: ROGUE DNS MONITOR

[Note: US patents 9,648,033 (Crume, 2017) and 9,225,731 (Crume, 2015) were split into separate patents by IBM attorneys in order to maximize legal protection and business value through the US Patent and Trademark Office. However, these are treated as one work for the purposes of this discussion. German patent 102013208923 (Crume, 2016) describes the same invention.]

5.2.3 Migration Across Authentication Systems

This invention (Crume, 2010) provides for a means to migrate users from one authentication system to another in a manageable, orderly process which avoids sending out new credentials to users and, thereby, minimizing the risk of compromise of those credentials. It also allows for groups of users to be migrated over time so as to minimize the impact to the system, the user community and the support staff that would need to intervene in failure cases. Perhaps most importantly, this invention allows the user to keep their existing password on the new system without violating the password expiry policy.

An administrator indicates a set of users to be migrated. When one of those designated users attempts to login to the system, the migration process begins. This approach creates two levels of staging to minimize disruption by migrating only a predetermined group of users at regular intervals and relying on the somewhat random timing of user logins to spread out the process further still.

When a user designated for migration logs in, the system saves the cleartext password entered and verifies the password against the old authentication system. Once authenticated, the user's password is then stored in the new authentication system and the user login process continues. After this time, the user will be authenticated only by the new system. In addition, the migration process also transfers the remaining password lifetime to the new system so that the password expiry interval is preserved across the migration process.

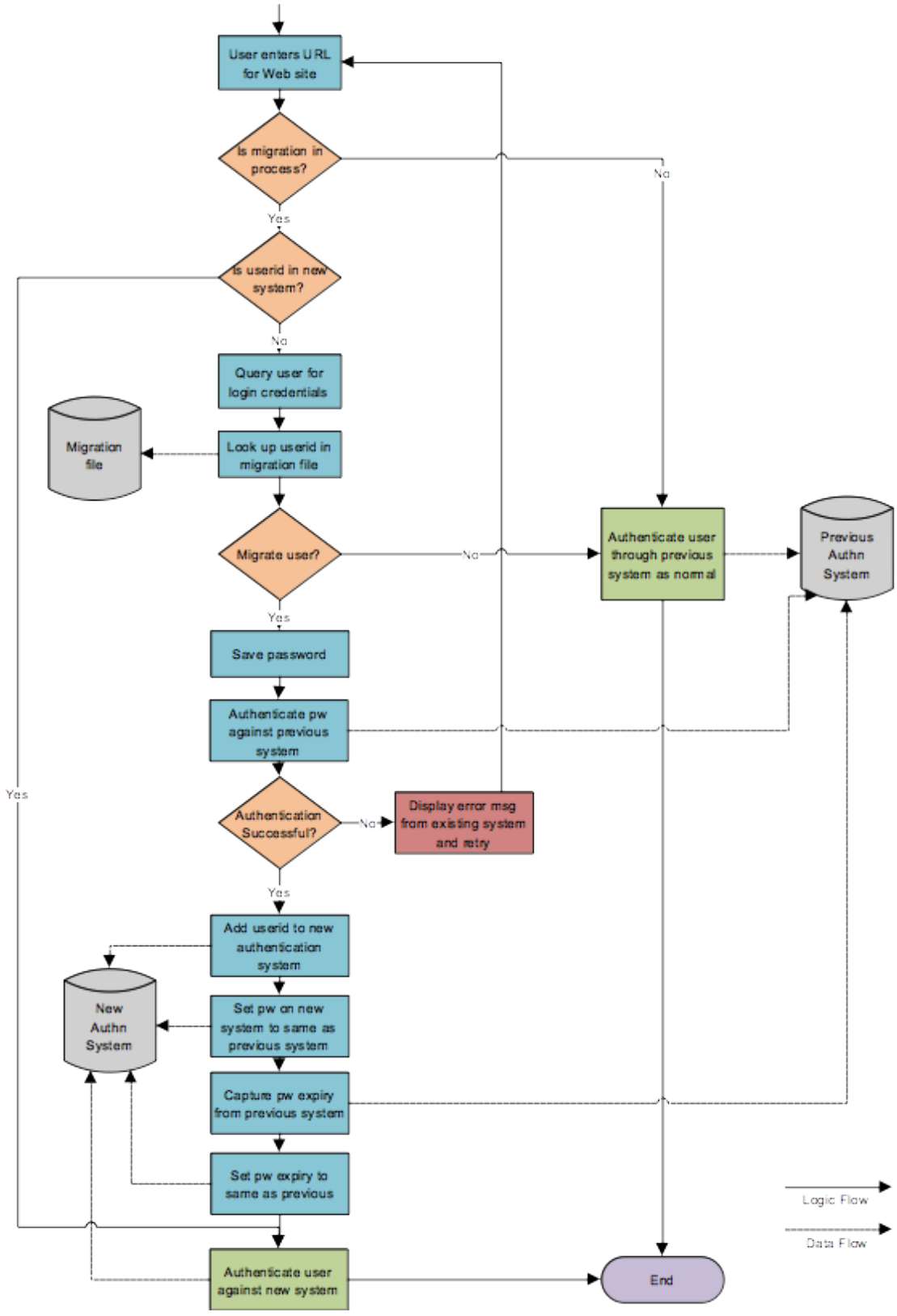


FIGURE 11: AUTHENTICATION SYSTEM MIGRATION FLOWCHART

5.2.4 Mobile Device Password Reset

US patents 9,088,896 and 9,078,135 describe an invention which allows an authorized user to securely regain full access to a locked mobile device for which they may have forgotten the password. The authorized user, while still able to unlock the device, must define a list of privileged phone numbers which can be used in the recovery process. These numbers will, presumably, belong to a group of trusted associates (or even other devices owned by the authorized user). These trusted devices can then aid in the recovery process.

To initiate this process the authorized user places a call (or has someone else place a call) to the locked device from one of the privileged devices. The authorized user confirms that the call is authentic because the Caller ID matches what is expected and answers the call and verifies the caller through their own innate ability to recognize the voice of the trusted caller. If the call is placed by an imposter, then the authorized user simply hangs up and the recovery process is ended. If the caller is recognized, the authorized user allows the call to continue until a predefined time interval has been exceeded. (Note: this delay allows the authorized user to determine the authenticity of the call.)

After the call threshold time has been exceeded, a message is displayed on the authorized user's phone asking if they want to reset their password. If this is desired, then the authorized user indicates this and terminates the call.

At this point the locked device automatically generates a temporary password and dials the privileged number that initiated the previous call. When the call is answered on the privileged device, that user will hear a machine-generated audible message telling them the temporary password and instructing them to enter it on their keypad. If this password is entered correctly, then the authorized user will be shown a password entry field where they can enter a new password and regain full access to their device.

[Note: US patents 9,088,896 (Bravo, et al., 2015) and 9,078,135 (Bravo, et al., 2015) were split into separate patents by IBM attorneys in order to maximize legal protection and business value through the US Patent and Trademark Office. However, these are treated as one work for the purposes of this discussion.]

5.3 Impact of Contributions

The works presented in this section build on the research previously cited in 5.1 Background and Related Works by improving security and flexibility. For example, (Fremberg, 2005) requires special, client-side software to be installed while the current work does not. (Peterson & Shaw, 2007) provides a means for migrating across authentication systems. The present work builds on this concept and provides additional features for staging the migration process so as to limit impact and preserves password expiration intervals. (Bravo, et al., 2015) improves on (Gillet & Mantyla, 2011) by having the locked device call back to the trusted device and then send the temporary password. This additional verification provides greater confidence that an attacker is not involved in the reset.

The approach presented here in (Crume, 2015) for passive monitoring offers some advantages over this approaches taken by (SB-Software, 2005) and others as follows:

- Passive monitoring does not introduce additional, superfluous network traffic as polling does (the latter being an approach used by other works)
- A passive monitor cannot be (easily) detected by the attacker, whereas a polling solution could be discovered when performing reconnaissance of the target network
- The polling approach only checks that known DNS servers are performing properly. The passive monitor described here is able to identify incorrect DNS resolutions coming from any host, making it useful in

detecting rogue DNS providers as these would not be known in advance and could, therefore, not be checked by the polling system.

The inventions described in this section have been the basis for subsequent research and inventions, as show in Tables 6-9. These consist of a total of 36 external citations from other companies such as Alibaba, Bank of America, Symantec, AT&T, Forbes, Juniper Networks, Cyber-Ark, Visa, Wells Fargo, Amazon, Audible and Tencent. These references include patents from the US, UK, Japan, China, Germany and the World International Property Organization (WIPO). In addition, to these external citations, this work has been used by the inventors as the basis for further enhancements as demonstrated through 2 self-citations. In addition, these external citations resulted in 149 forward citations to yet other works.

TABLE 6: CITATIONS FOR US# 8,533,821 DETECTING AND DEFENDING AGAINST MAN-IN-THE-MIDDLE ATTACKS

Publication number	Assignee	Year	Forward Citations (102)	Title
External Citations (24)				
CN104239758B	阿里巴巴集团控股有限公司	2018	8	A human-machine identifying method and corresponding CAPTCHA
CN104519018B	阿里巴巴集团控股有限公司	2018	9	A method of preventing a malicious for the server request method, apparatus and system for
CN105516066A	阿里巴巴集团控股有限公司	2016	0	Method and device for identifying existence of intermediary
CN106357628A	东软集团股份有限公司	2017	0	Attack defense method and device
DE102014222219A1	Robert Bosch Gmbh	2016	0	Method and apparatus for authentication of a device
JP5088403B2	横河電機株式会社	2012	17	Improper communication detection system
US20130311784A1	Micheal Bleahen	2013	4	System and method for preventing unauthorized access to information
US20140283049A1	Bank of America Corporation	2014	6	Handling information security incidents
US20150135327A1	Symcor Inc.	2015	1	Method of obfuscating relationships between data in database tables
US20170006060A1	Symantec Corporation	2017	0	Systems and methods for detecting man-in-the-middle attacks
US8356333B2	Bespoke Innovations Sarl	2013	21	System and method for verifying networked sites
US8595829B1	Symantec Corporation	2013	4	Systems and methods for automatically blacklisting an internet domain based on the activities of an application
US8973140B2	Bank of America Corporation	2015	6	Handling information security incidents
US9083730B2	AT&T Intellectual Property I., L.P.	2015	3	Methods and apparatus to identify an internet protocol address blacklist boundary

US9356845B1	Forbes Media Llc	2016	0	System and method for audience segment profiling and targeting
US9438494B2	Avvasi Inc.	2016	10	Apparatus and methods for optimizing network data transmission
US9443068B2	Micheal Bleahen	2016	4	System and method for preventing unauthorized access to information
US9553882B2	Empire Technology Development Llc	2017	0	Correlation of advertising content to malicious software
US9722801B2	Juniper Networks, Inc.	2017	6	Detecting and preventing man-in-the-middle attacks on an encrypted connection
US9800589B1	Sonus Networks, Inc.	2017	0	Methods and apparatus for detecting malicious attacks
US9888035B2	Symantec Corporation	2018	0	Systems and methods for detecting man-in-the-middle attacks
WO2016178088A2	Cyber-Ark Software Ltd.	2016	3	Systems and methods for detecting and reacting to malicious activity in computer networks
WO2018023466A1	步晓芳	2018	0	Account input method and browser
WO2018169522A1	Visa International Service Association	2018	0	Method and system for relay attack detection
Self-Citations (1)				
US10169759B2	IBM Corp	2019		Verifying online transaction integrity and authentication with QR codes

TABLE 7: CITATIONS FOR US# 9,225,731 DETECTING THE PRESENCE OF ROGUE DOMAIN NAME SERVICE PROVIDERS

Publication number	Assignee	Year	Forward Citations (14)	Title
External Citations (6)				
GB2518460B	F Secure Corp	2015	5	Unauthorised/Malicious redirection
CN105338123B	国际商业机器公司	2018	4	A method for resolving a domain name in a network, devices and systems
CN104168339A	汉柏科技有限公司	2014	4	Method and device for preventing domain name from being intercepted
US10230743B1	Wells Fargo Bank, N.A.	2019	0	Rogue endpoint detection
CN106060067B	上海交通大学	2018	1	Malice domain name detection method based on Passive DNS iteration cluster
CN108156262A	中国联合网络通信集团有限公司	2018	0	Method and device for inspecting effectiveness of DNS (domain name system) configuration files
Self-Citations (1)				
US20130318605A1	IBM Corp	2013		System for detecting rogue network protocol service providers

TABLE 8: CITATIONS FOR US2010/0269151A1 MIGRATION ACROSS AUTHENTICATION SYSTEMS

Publication number	Assignee	Year	Forward Citations (25)	Title
External Citations (2)				
US9819669B1	Amazon Technologies, Inc.	2017	0	Identity migration between organizations
US9112844B2	Audible, Inc.	2015	25	Device credentialing for network access

TABLE 9: CITATIONS FOR US# 9,078,135 MOBILE DEVICE RESET

Publication number	Assignee	Year	Forward Citations (8)	Title
External Citations (4)				
US9355244B2	Tencent Technology (Shenzhen) Company Limited	2016	4	Systems and methods for password reset
CN104808934A	富泰华工业（深圳）有限公司	2015	4	Electronic equipment and unlocking control method thereof
CN105786303A	纬创资通（中山）有限公司	2016	0	Screen unlocking method of electronic device, and electronic device
CN106503539A	公安部第三研究所	2017	0	Screen lock password cracking method and evidence acquisition system for intelligent equipment based on Mobex protocol

6 CONCLUSION

MITM attacks are one of the more problematic areas within the realm of Cybersecurity. If imposters are able to insert themselves into the communication path between two legitimate parties, personal details (including passwords and credit card numbers) as well as sensitive organizational information may be divulged and transactions altered. The key to defeating MITM attacks begins with strong authentication capabilities which ensure that the parties are, in fact, communicating with who they believe they are communicating with.

This Integrative Summary has provided a description of contributions broadly in the field of Identity and Access Management with a focus more specifically in the area of authentication solutions and improvements in that space. This research is realized through a series of patent filings, which enhance the areas of user-centric and transaction-centric authentication. These inventions further the goal of creating greater levels of confidence and trust through additional mechanisms, including out of band communications, expected user location and geolocation correlation. Each of these inventions help to ensure that the parties are who they claim to be and that transaction details have not been tampered with by an MITM.

Further still, enhancements to the capabilities which support the authentication system have also been presented. These include a process which provides nondisruptive migration across authentication systems, a mechanism for securely regaining control of a mobile device for which the password has been lost and features which detect attempts to subvert the integrity of the underlying networking infrastructure.

The research presented here spans a number of years during which time the threat of MITM attacks has increased, making this work even more relevant. Evidence of this can be seen from the fact that these patents have been cited by 79 other patents held by many innovative, high profile tech companies from around the world. Further, those patents have been cited by another 398 patents bringing the total of external works influenced to 477 at the time of this writing. Also, the individual works build on each other, as presented in Section 2, comprising an additional 18 self-citations among the body of research. Figure 12: Citation Map illustrates these relationships with the IBM Corp nodes representing the patents that form the basis for this thesis.

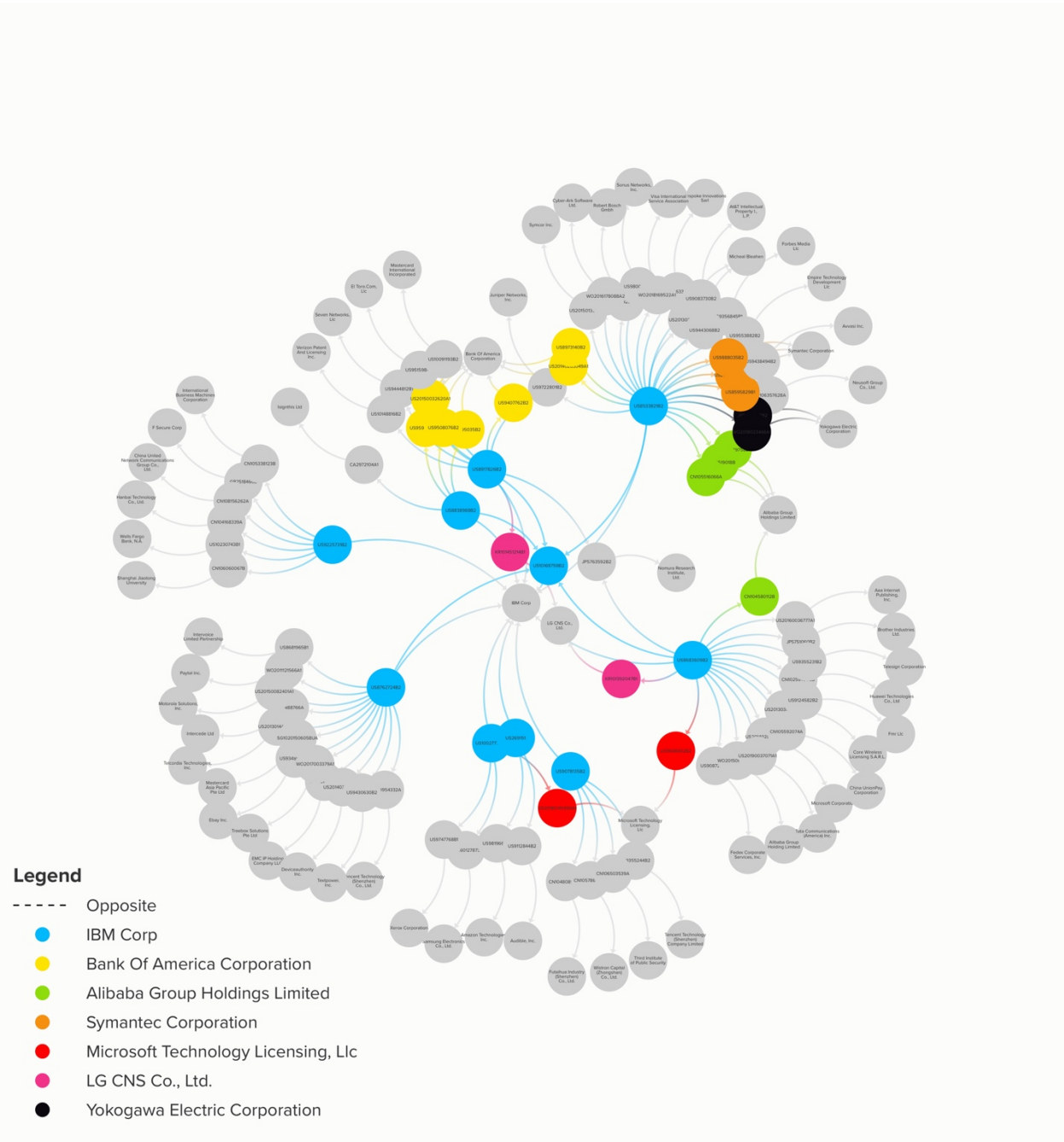


FIGURE 12: CITATION MAP

However, limitations remain in this area as attackers continue to find ways to compromise the authentication system. Any system that relies on passwords will always run the risk that this knowledge is not exclusive and has been either shared or stolen. Mobile devices can be compromised with malware that intercepts authentication challenges and either actively intercedes or passively monitors communications. Also, despite the best technology, human error on the part of unsuspecting or uneducated users will be exploited by attackers.

Future research should seek to further reduce the impact of these vulnerabilities. A focus on risk-based authentication and graded trust which moves beyond a simple “allow” or “deny” access determination, but which provides greater degrees of access based upon higher degrees of confidence is needed. Now that so many people carry mobile devices, which have reasonably strong embedded biometric readers, a move away from the use of passwords by users and toward multi-factor authentication could improve both security and usability – a rare win-win in the security space between two objectives that are often in conflict.

Follow-on efforts should look to improve both the accuracy and convenience of biometric systems while not compromising user privacy. Challenges have arisen in recent years where conflicting desires by vendors to assure users that their mobile devices are secure while law enforcement seeks backdoors that would allow them access. Technical solutions that balance these competing goals have proven difficult since a backdoor for some could prove to be a backdoor for all. Therefore, security researchers should also look explore areas of public policy and education as areas for future developments as well.

Finally, some of the inventions comprising this research leverage SMS messaging and telephony voice calls as an out of band communications channel, which the MITM attacker would not have access to. However, as mobile device malware and surveillance software continues to develop, even these channels could be compromised by an attacker who has managed to establish a foothold on the device. The development of new mechanisms which are not vulnerable to this scenario is needed and should be the focus of future research.

7 REFERENCES

Adams, A. & Sasse, M. A., 1999. Users Are Not the Enemy. *Communications of the ACM,* 42(12), pp. 41-46.

Adida, B., n.d. *BeamAuth: Two-Factor Web Authentication with a Bookmark.* s.l.:s.n.

Alicherry, M. & Angelos, K., 2009. *DoubleCheck: Multi-path Verification Against Man-in-the-Middle Attacks,* New York, NY, USA: IEEE.

Belenguer, J. & Calafate, C., 2007. *A low-cost embedded IDS to monitor and prevent Man-in-the-Middle attacks on wired LAN environments.* Valencia, Spain, The International Conference on Emerging Security Information, Systems, and Technologies.

Bonneau, J., 2012. The science of guessing: analyzing an anonymized corpus of 70 million passwords. *IEEE Symposium on Security and Privacy,* pp. 538-552.

Bravo, J. & Covalla, T., 2006. *Methods and Apparatus for Restricting Access of a User Using a Cellular Telephone.* USA, Patent No. 7,133,662.

Bravo, J. & Crume, J., 2008. *Method of and System for Strong Authentication and Defense Against Man-in-the-Middle Attacks.* USA, Patent No. US 2008/0318548 A1.

Bravo, J. & Crume, J., 2014. *Detecting Man-in-the-Middle Attacks in Electronic Transactions Using Prompts.* USA, Patent No. 8,917,826.

Bravo, J. & Crume, J., 2014. *Mobile Phone and IP Address Location Correlation Service.* USA, Patent No. 8.683,609.

Bravo, J. & Crume, J., 2014. *Verification of Transactional Integrity.* USA, Patent No. 8,838,988.

Bravo, J. & Crume, J., 2014. *Website Authentication.* USA, Patent No. 8,762,724.

Bravo, J. & Crume, J., 2017. *Verifying Online Transaction Integrity and Authentication with QR Codes.* USA, Patent No. US 10,169,759 B2.

Bravo, J. & Crume, J., 2018. *Expected Location-based Access Control.* USA, Patent No. 10,027,770.

Bravo, J., Crume, J. & Hinds, N., 2015. *Mobile Device Password Reset.* USA, Patent No. 9,088,896.

Bravo, J., Crume, J. & Hinds, N., 2015. *Mobile Device Reset.* USA, Patent No. 9,078,135.

Bryan, D. & Heywood, D., 2017. *The 'Cracken' in Action: A Password Cracking Adventure.* [Online] Available at: https://securityintelligence.com/the-cracken-in-action-a-password-cracking-adventure/

Bryan, D. & Heywood, D., 2018. *Passwords Suck: Using Cracken to Break Passwords at the Speed of Billions of Hashes Per Second.* [Online]
Available at: https://www.ibm.com/events/think/watch/replay/113883943/

Burkholder, P., 2002. *SSL Man-in-the-Middle Attacks.* [Online]
Available at: https://www.sans.org/reading-room/whitepapers/threats/ssl-man-in-the-middle-attacks-480

Bychkov, E., 2007. *Entended One-Time Password Method and Apparatus.* USA, Patent No. US 2007/0067828 A1.

Calabrese, G. & Stemer, W., 2008. *Mobile Phone Charge Card Notification and Authorization Method.* USA, Patent No. 7,357,310.

Callegati, F., Cerroni, W. & Ramilli, M., 2009. Man-in-the-Middle Attack to the HTTPS Protocol. *IEEE Security & Privacy*, 3 February, pp. 78-81.

Camaisa, A. & Samuelsson, J., 2007. *System and Method for Blocking Unauthorized Network Log In Using Stolen Password.* USA, Patent No. US 2007/0266257 A1.

Carli, F., 2003. *Security Issues with DNS.* SANS Reading Room: https://www.sans.org/reading-room/whitepapers/dns/paper/1069.

Chesire, S., 2006. *Method and Apparatus for Detecting Incorrect Responses to Network Queries.* USA, Patent No. US 2006/0253612 A1.

Clough, I., 2007. *Method and System for Enhanced Security Using Location-based Wireless Authentication.* USA, Patent No. 7,221,949.

Constable, C., 2008. *Method and System for Dynamically Controlling Access to a Network.* USA, Patent No. US 2008/0189776 A1.

Conti, M., Dragoni, N. & Lesyk, V., 2016. A Survey of Man In The Middle Attacks. *IEEE Communications Surveys & Tutorials,* 18(3), pp. 2027-2051.

Crilly Jr., W., 2005. *Detecting Wireless Interlopers.* USA, Patent No. US 2005/0075070 A1.

Crume, J., 2000. In: *Inside Internet Security: What Hackers Don't Want You to Know.* s.l.:Addison-Wesley, pp. 102-122.

Crume, J., 2010. *Migration Across Authentication Systems.* USA, Patent No. US2010/0269151A1.

Crume, J., 2013. *Detecting and Defending Against Man-in-the-Middle Attacks.* USA, Patent No. 8,533,821.

Crume, J., 2013. *Detecting and Defending Against Man-in-the-Middle Attacks.* USA, Patent No. 8,522,349.

Crume, J., 2014. Identity and Access Management Architecture. In: R. O'Hanley & J. Tiller, eds. *Information Security Management Handbook (Sixth edition, Volume 7).* Boca Raton, FL, USA: CRC Press, pp. 221-238.

Crume, J., 2015. *System for Detecting the Presence of Rogue Domain Name Service Providers through Passive Monitoring.* USA, Patent No. 9,225,731.

Crume, J., 2016. *System zum Erfassen des Vorhandenseins eines bösartigen Domain-Name-Service-Providers durch passive Überwachung.* Germany, Patent No. DE 10 2013 208 923 B4.

Crume, J., 2017. *System for Detecting the Presence of Rogue Domain Name Service Providers through Passive Monitoring.* USA, Patent No. 9,648,033.

Denning, D. & MacDoran, P., 1998. Location-based authentication: grounding cyberspace for better security. In: *Internet Besieged.* New York, NY: ACM Press/Addison-Wesley Publishing Co., pp. 167-174.

Dewe, C. et al., 2009. *Authentication Methods and Systems.* USA, Patent No. US2009/0300738 A1.

Doyle, R., Hind, J., Mannaru, D. & Vellanki, V., 2006. *Method, System, Service, and Computer Program Product for Identifying Incorrect Domain Name to Internet Protocol (IP) Address Mappings.* USA, Patent No. US 2006/0176822 A1.

Ellison, C. & Schneier, B., 2000. *Ten Risks of PKI: What You're Not Being Told About Public Key Infrastruture.* [Online] Available at: https://www.schneier.com/academic/paperfiles/paper-pki.pdf

Felt, A.; et al, 2015. *Improving SSL Warnings: Comprehension and Adherence.* Seoul, Republic of Korea, Association for Computing Machinery, p. https://ai.google/research/pubs/pub43265.

Franken, Z., 2007. *Biometric and token based access control systems: Are you protected by two screws and a plastic cover? Probably.* [Online]
Available at: https://www.defcon.org/html/links/dc-archives/dc-15-archive.html#Franken
[Accessed September 2018].

Fremberg, D., 2005. *Authentication Protocol.* USA, Patent No. US 2005/0022020 A1.

Gillet, E. & Mantyla, J., 2011. *Method and apparatus for User Interaction While Device is Locked.* USA, Patent No. US 2011/0159844 A1.

Goldberg, I. & Boaz, M., 2013. *Security for Future Log-on Location.* USA, Patent No. US 2013/0055370 A1.

GSMA Intelligence, 2017. *Global Mobile Trends 2017,*
https://www.gsmaintelligence.com/research/?file=3df1b7d57b1e63a0cbc3d585feb82dc2&utm_source=Triggermail&utm_medium=email&utm_campaign=Post%20Blast%20%28bii-apps-and-platforms%29:%20Apple%20drops%20in-app%20tipping%20tax%20—%20Two-thirds%20of%20the%20globe: GSMA Intelligence.

Hadizad, P., 2014. *System and method for Unlocking an Electronic Device Via a Securely Paired Remote Device.* USA, Patent No. US 2014/0085048 A1.

Heywood, D., 2017. *Advanced Password Recovery with Hashcat* [Interview] 2017.

Jalalzai, M., Shahid, W. & Iqbal, M., 2015. DNS security challenges and best practices to deploy secure DNS with digital signatures. *IEEE Xplore,* 12 March.978-1-4799-6369-0(https://ieeexplore.ieee.org/document/7058517).

Jaros, D. & R., K., 2010. *New Location-based Authentication Techniques in the Access Management.* Valencia, Spain, IEEE Xplore, 2010 Sixth International Conference on Wireless and Mobile Communications.

Jenkins, J. e. a., 2016. *More Harm Than Good? How Messages That Interrupt Can Make Us Vulnerable.* [Online] Available at: https://pubsonline.informs.org/doi/10.1287/isre.2016.0644#

Jones, J. et al., 2008. *Mobile Payment System and Method.* USA, Patent No. US 2008/0270301 A1.

Kato, T., 2013. *Authentication System, Authentication Method and Authentication Server.* USA, Patent No. US 2013/0109351 A1.

Kermode, A., 2009. *Using a human readable code communicated using a trusted channel to verify that a distributed public key was issued by the party who claims to have issued it.* Great Britian, Patent No. GB 2,456,509.

Kiliccote, H., 2008. *Method and Apparatus for Providing Authentication.* USA, Patent No. 7,379,921.

Kiliccote, H., 2008. *Method and Apparatus for Providing Secure Document Distribution.* USA, Patent No. 7,380,708.

Law, S., Hapuarachchi, B., Tse, D. & Law, J., 2008. *Secure Wireless Authorization System.* USA, Patent No. 7,447,494.

Lee, S. & Choi, Y., n.d. *A Resilient Packet-Forwarding Scheme against Maliciously Packet-Dropping Nodes in Sensor Networks.* s.l.:Dept. of Computer Engineering, Hongik University.

Leung, C., n.d. *Depress Phishing by CAPTCHA with OTP,* Hong Kong: s.n.

Mahato, A., Kumar, A. & Singh, A., 2014. Mobile Phone Cloning. *International Journal for Research in Applied Science and Engineering Technology,* 2(IX), pp. 224-228.

Morris, R. & Thompson, K., 1979. Password Security: A Case History. *Communications of the ACM,* 22(11), pp. 594-597.

Niedermeyer, B., 2008. *Location Based Fraud Reduction System and Method.* USA, Patent No. 7,376,431.

O'Gorman, L., 2003. Comparing Passwords, Tokens, and Biometrics for User Authentication. *Proceedings of the IEEE,* 91(12), pp. 2021-2040.

Olson, E. & Ogorek, G., 2009. *Method and System for Discovering DNS Resolvers.* USA, Patent No. US 2009/0327487 A1.

O'Neil, J., 2002. *Efficient and Secure Bill Payment via Mobile IP Terminals.* USA, Patent No. US 2002/0069165 A1.

Patel, K., Han, H., Jain, A. & Ott, G., 2015. *Live Face Video vs. Spoof Face Video: Use of Moire´ Patterns to Detect Replay Video Attacks.* Phuket, Thailand, International Conference on Biometrics.

Peterson, M. & Shaw, J., 2007. *Apparatus System and Method for Real-time Migration of Data Related to Authentication.* USA, Patent No. US 2007/0083917 A1.

Rados, S. et al., 2009. *Two Factor Authentication for Financial Transactions.* USA, Patent No. 7,600,676 B1.

SB-Software, 2005. *DNS Watcher.* [Online]
Available at: http://www.sb-software.com/dnswatcher/

Seifried, K., 2000. *"The End of SSH and SSL? Follow-up".* [Online]
Available at: www.seifried.org/security/cryptography/20011108-sslssh-followup.html

Seifried, K., 2000. *"The End of SSH and SSL?".* [Online]
Available at: www.seifried.org/security/cryptography/20011108-end-of-ssl-ssh.html

Shan, A., Weiyin, R. & Shoulian, T., 2008. *Analysis and Reflection on the Security of Biometrics System.* Dalian, China, 4th International Conference on Wireless Communications, Networking and Mobile Computing.

Shaobu, M., 2011. *Method and Device for Preventing Domain Name Spoofing.* USA, Patent No. US 2011/0231931 A1.

Smith, D., Wiliem, A. & Lovell, B., 2015. Face Recognition on Consumer Devices: Reflections on Replay Attacks. *IEEE Transactions on Information Forensics and Security,* 10(4), pp. 736-745.

Steinberg, J., 2007. *System and Method of Using Two or More Multi-factor Authentication Mechanisms to Authenticate Online Parties.* USA, Patent No. US 2007/0136573 A1.

Stoll, J., Tashman, C., Edwards, K. & Spafford, K., 2008. Sesame: Informing User Security Decisions with System Visualization. *CHI 2008 Proceedings - Am I Safe.*

Sunshine, J. et al., 2009. *"Crying Wolf: An Empirical Study of SSL Warning Effectiveness".* [Online] Available at: https://www.usenix.org/legacy/event/sec09/tech/full_papers/sunshine.pdf

Tabassum, K., 2017. *An Efficient Authentication Technique for Security Management Against Cloning Mobile Phones.* Poonamalee, Tamil Nadu, India, International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS-2017).

The MITRE Corporation, 2018. *CAPEC-94: Man in the Middle Attack.* [Online]
Available at: http://capec.mitre.org/data/definitions/94.html
[Accessed 17 October 2018].

Thompson, I., 2017. *Archive of 1.4 billion credentials in clear text found in dark web archive.* [Online]
Available at:
https://www.theregister.co.uk/2017/12/12/1_point_4_billion_credentials_in_clear_text_in_dark_web_archive/

Turnbull, R. & Gedge, R., 2006. *Location Based Authentication.* World Intellectual Property Organization, Patent No. WO 2006/103387 A1.

Ur, B. et al., 2015. *Measuring Real-World Accuracies and Biases in Modeling Password Guessability.* Washington, DC, 24th USENIX Security Symposium.

Wagner, R. & Bryner, J., 2001. *Address Resolution Protocol Spoofing and Man-in-the-Middle Attacks.* [Online] Available at: https://www.sans.org/reading-room/whitepapers/threats/address-resolution-protocol-spoofing-man-in-the-middle-attacks-474

Wahl, M., 2010. *System and Method for Calenar-based Anomalous Access Detection.* USA, Patent No. 7,747,645.

8 LIST OF PUBLISHED WORKS

The following list of published works contain the body of research that is the basis for this thesis. In addition, the results from the prior art searches conducted by outside, independent legal counsel as part of the patent filing process along with responses, which document the novelty of the inventions, are included. (Note: The differentiation comments included here are based upon *adapted* versions of the correspondence that was exchanged with legal counsel. The text has been edited down to the key points of relevance for each response, consolidating responses from multiple inventors, where appropriate).

8.1 INFORMATION SECURITY MANAGEMENT HANDBOOK

Identity and Access Management Architecture

- Crume, J., 2014. Identity and Access Management Architecture. In: R. O'Hanley & J. Tiller, eds. *Information Security Management Handbook (Sixth edition, Volume 7).* Boca Raton, FL, USA: CRC Press, pp. 221-238.

Research Contribution

This book chapter provides a holistic framework for identity and access management, which forms the basis upon which this work in the area of authentication is based.

Author's Contribution

Jeff Crume was the sole author of this work.

8.2 WEBSITE AUTHENTICATION PATENT

- Bravo, J. & Crume, J., 2014. *Website Authentication.* USA, Patent No. 8,762,724.

Research Contribution

This US patent provides a greater level of assurance that a user is who they claim to be through verification of an OTP via an OOB communications channel.

Author's Contribution

Jeff Crume and Jose Bravo collaborated on this patent. Both contributed to this work by developing and refining the idea, documenting the invention, defending the submission before the IBM Invention Disclosure Board, reviewing and providing commentary regarding similar prior art and reviewing the final patent filing.

Differentiation response from 13 October 2008

- **US2007/0266257 A1 System and Method for Blocking Unauthorized Network Log in Using Stolen Password:** This involves the use of browser cookies which limit its applicability to using the same browser for each session. The present invention does not have this limitation. Further, this approach described here requires the user to memorize a pre-determined secret, which is then used as the basis for the user to recognize the site. The present invention presents a unique, one-time password (OTP) with each log in with no memorization required.

- **US2008/0181380 A1 Proxy for Authenticated Caller Name:** This is limited to phone calls where the present invention is extensible to Web, ATM or other transactions. Also, this prior art authenticates the user to the system where the present invention authenticates the system to the user.
- **US 7,379,921 B1 Method and Apparatus for Providing Authentication:** This involves the use of images for authentication. The present invention uses an OTP, which can subsequently be entered into a telephone keypad providing greater portability with no prior knowledge required by the user.
- **US 7,380,708, B1 Method and Apparatus for Providing Secure Document Distribution:** Same as previous**.**
- **Sesame: Informing User Security Decisions with System Visualization (Stoll, J. et al):** Same as previous**.**
- **Holistic VoIP Intrusion Detection and Prevention System (Nassar, M., et al):** This deals with authentication of a voice over an IP telephony infrastructure and is focused on intrusions rather than authentication.
- **BeamAuth: Two-Factor Web Authentication with a Bookmark (Adida, B.):** This deals with web authentication only with no out of band process and is limited to browsers with JavaScript support. The present invention does not have these limitations.
- **Getting Users to Pay Attention to Anti-phishing Education: Evaluation of Retention and Transfer (Kumaraguru, P., et al):** This deals with a training methodology rather than an actual phishing detection mechanism as is the case with the present invention.

8.3 Mobile Phone and IP Address Location Correlation Service

- Bravo, J. & Crume, J., 2014. *Mobile Phone and IP Address Location Correlation Service.* USA, Patent No. 8.683,609.

Research Contribution

This US patent provides a means for detecting the presence of an MITM, who might, otherwise, be able to compromise the integrity of a transaction or impersonate a legitimate user.

Author's Contribution

Jeff Crume and Jose Bravo collaborated on this patent. Both contributed to this work by developing and refining the idea, documenting the invention, defending the submission before the IBM Invention Disclosure Board, reviewing and providing commentary regarding similar prior art and reviewing the final patent filing.

Differentiation response from 19 June 2009

- **US20080189776A1 Method and System for Dynamically Controlling Access to a Network:** This is not applicable within the context of a mobile phone being used as a strong authentication factor. Further, it describes a system which would receive location information as input whereas the current invention describes a system in this information is actually derived and compared to a specified range.
- **US20080318548A1 Method of and System for Strong Authentication and defense against man-in-the-middle attacks:** The present invention actually complements this prior art, which was developed by the same inventors, by allowing the correlation service to provide an indication as to location match without having to reveal full location details, thereby, preserving privacy.
- **WO2008147353A1 Method and system for authenticating internet user identity:** This prior art does not deal with the context of a mobile phone used as a second factor for authentication, as the present invention does.
- **WO04079499A2 System and method for verifying user identity:** Same comments as above

- **US7360248 Methods and apparatus for verifying the identity of a user requesting access using location information:** This relies on GPS, which may be inaccessible inside a building and would be a severe limitation. The present invention can use cell tower triangulation which, while not as precise, will work inside and should be exact enough for the intended purposes.
- **US7376431 Methods and apparatus for verifying the identity of a user requesting access using location information:** This involves the use of specialized tracking devices which the present invention does not require.
- **US20020069165A1 Efficient and secure bill payment via mobile IP terminals:** This does not leverage a mobile phone as a second authentication factor. Further, this invention relies on the use of a special localized network where all accesses must be performed. By contrast, the present invention works across the general purpose, public Internet.
- **US20090094682A1 Methods and systems for user authorization:** This focuses on role-based authentication which the present invention does not deal with.
- **WO06103387A1 Location based authentication:** This invention only applies to a restricted, previously designated workspace. The present invention can work essentially anywhere a mobile phone signal is available.
- **US7221949 Method and system for enhanced security using location-based wireless authentication:** This invention requires the use of new data flows and changes to message formats. The present invention describes a separate service which does not interfere with the mainline data flows.

8.4 Detecting Man-in-the-Middle Attacks Using Geolocation and Voice Response Telephony Prompts

- Bravo, J. & Crume, J., 2014. *Detecting Man-in-the-Middle Attacks in Electronic Transactions Using Prompts.* USA, Patent No. 8,917,826.

Research Contribution

This US patent builds on the previous works by providing a mechanism for detecting an MITM by leveraging both an OTP and geolocation information.

Author's Contribution

Jeff Crume and Jose Bravo collaborated on this patent. Both contributed to this work by developing and refining the idea, documenting the invention, defending the submission before the IBM Invention Disclosure Board, reviewing and providing commentary regarding similar prior art and reviewing the final patent filing.

Differentiation response from 20 September 2011

- **GB 2 456 509 A Using a Human readable code communicated using a trusted channel to verify that a distributed public key was issued by the party who claims to have issued it:** This invention involves verification of public keys and does not utilize either mobile or land line telephony.
- **DoubleCheck: Multi-path Verification Against Man-in-the-Middle Attacks (Alicherry, M., et al):** This does not use telephony but rather involves certificate retrieval for verification.
- **US 2009/0300738 A1 Authentication Methods and Systems:** This requires an app be downloaded to the mobile device in order to perform cryptographic functions, which the present invention does not require.

- **VoIP Interception in P2P SIP Environment (Kooi, T., et al):** This paper demonstrates how interception can happen in voice over IP telephony but does not present a strong authentication solution as of the type described in the present invention.
- **Depress Phishing by CAPTCHA with OTP (Leung, C., et al):** This paper refers to the use of both CAPTCHAs and One Time Passwords, neither of which are leveraged by the present invention.
- **US 2007/0067828 A1 Extended One-Time Password and Apparatus:** The present invention is not dependent upon OTPs as this one is.
- **US 2007/0136573 A1 System and method of using two or more multi-factor authentication mechanisms to authenticate online parties:** The present invention is not dependent upon OTPs as this one is.
- **US 2007/0266257 A1 System and method for blocking unauthorized network log in using stolen password:** This work provides a means for a user to determine if a web site is authentic. The present invention does the reverse.
- **US 2009/0106138 A1 Transaction authentication over independent network:** The present invention is not dependent upon OTPs as this one is.
- **US 2010/0269162 A1 Website Authentication:** This present invention builds on this one by the same inventors by providing greater assurance that the user is who they claim to be (rather than the reverse).
- **US 2011/0154459 A1 Method and system for securing electronic transaction:** This invention involves storing credentials in a vault, which the present invention does not use.
- **US 2011/0197070 A1 System and method for in- and out-of-band multi-factor server-to-user authentication:** This invention uses a random subset of predefined locations in the server path, which the present invention does not focus on.
- **US 7,840,993 B2 Protecting one-time-passwords against man-in-the-middle attacks:** This invention uses cryptographic techniques to secure an OTP. The present invention involves neither technology.
- **Voice Interactive Personalized Security (VoIPSEC) protocol (Kopsidas, S., et al):** This paper describes a system which leverages biometrics, which are not part of the present invention.

8.5 Expected Location-based Access Control

- Bravo, J. & Crume, J., 2018. *Expected Location-based Access Control.* USA, Patent No. 10,027,770.

Research Contribution

This US patent provides a means for greater confidence in the authentication process by verifying that a user is who they claim to be by ensuring that they are where they expected to be from a geolocation perspective.

Author's Contribution

Jeff Crume and Jose Bravo collaborated on this patent. Both contributed to this work by developing and refining the idea, documenting the invention, defending the submission before the IBM Invention Disclosure Board, reviewing and providing commentary regarding similar prior art and reviewing the final patent filing.

Differentiation response from 5 November 2013

- **US 2013/0109351 Authentication system, authentication method and authentication server:** This invention is designed for use with ATMs which have a known, fixed location and not with end users who may be mobile.

- **US 7,747,645 B2 System and Method for calendar-based anomalous access detection:** This invention relies only on calendar entries as the source for expected user location. The present invention is written more broadly to include other sources. One important source includes a user's travel itineraries from a travel agent or provider. The present invention also extends to include work schedules (e.g. for shift workers) and vacation schedules.
- **US 2013/0055370 A1 Security for Future Logon Location:** This work relies on past logins to predict where a user might log in next. It also considers the distance between the current login location and the previous one to determine if the user could, in fact, have traveled that distance in the time that elapsed between the two. The present invention uses network information only to determine current location -- not previous or future.

8.6 VERIFICATION OF TRANSACTIONAL INTEGRITY

- Bravo, J. & Crume, J., 2014. *Verification of Transactional Integrity.* USA, Patent No. 8,838,988.

Research Contribution

This US patent provides a means for ensuring that transaction details have not been tampered with by an MITM. It does this by speaking these details to the user via a phone call to a designated number.

Author's Contribution

Jeff Crume and Jose Bravo collaborated on this patent. Both contributed to this work by developing and refining the idea, documenting the invention, defending the submission before the IBM Invention Disclosure Board, reviewing and providing commentary regarding similar prior art and reviewing the final patent filing.

Differentiation response from 15 Dec 2010

- **US 2008/027301 A1 Mobile Payment System and Method:** This involves having the user call the service provider first to initiate the transaction with the mobile device used for verification. The present invention does essentially the reverse where the transaction is initiated online (via web browser, ATM or mobile device) and a voice call is used to confirm the integrity of the transaction.
- **US 2008/0318548 A1 Method of and System for Strong Authentication and Defense Against Man-in-the-Middle Attacks:** The present invention builds on this prior art from the same inventors and could be used together to improve security. The prior invention is focused on authenticating the user via geo location matching of the mobile device and the IP address whereas the present invention deals with details of the actual transaction.
- **US 2010/0051686 A1 System and Method for Authenticating a Transaction Using a One-Time Pass Code:** This involves authenticating the user via a one-time passcode generated by the mobile device. The present invention verifies transaction details after authentication has already occurred and does not rely on a one-time passcode and can, therefore, work with any telephony device – not just a smart phone.
- **US 7,357,310 B2 Mobile Phone Charge Card Notification and Authorization:** This does involve verifying transaction details but does it through entering a one-time passcode on the mobile device. The present invention uses an out of band phone call where transaction details are read audibly to the user for verification.
- **US 7,447,494 B2 Secure Wireless Authorization System:** Essentially the same distinction as the previous invention.

- **US 7,600,676 B1 Two Factor Authentications for Financial Transactions:** Also similar to the two previous inventions but focused on authentication while the present invention deals with verification of transaction integrity. Further, this prior art relies on SMS messaging, which can be spoofed.

8.7 Verification of Transactional Integrity and Authentication with QR Codes

- Bravo, J. & Crume, J., 2017. *Verifying Online Transaction Integrity and Authentication with QR Codes.* USA, Patent No. US 10,169,759 B2.

Research Contribution

This US patent builds on the previous work and adds QR codes as a means to transmit transaction details.

Author's Contribution

Jeff Crume and Jose Bravo collaborated on this patent. Both contributed to this work by developing and refining the idea, documenting the invention, defending the submission before the IBM Invention Disclosure Board, reviewing and providing commentary regarding similar prior art and reviewing the final patent filing.

Differentiation response from 22 May 2015

- **US 2013/0086650 Communication System Including Optical Recognition and Method of Using Same:** This involves a communication system which could be used to pass calls from one device to another. It is not designed to deal with security threats or to verify the integrity of transactions.
- **US 2015/0099758 Authenticating Users to ATMs and Other Secure Machines for Cardless Transactions:** This invention is limited to authenticating a user to the system. It does not deal with attacks on the integrity of subsequent transaction details.
- **JP2008152737A Service Provision Server, Authentication Server and Authentication System:** This invention is limited to authenticating a user to the system. It does not deal with attacks on the integrity of subsequent transaction details.
- **WO 2014/122614 A2 A Secure User Interaction Method Performing Defined Actions no Web Resources over a Separate Channel and a System Thereof:** This invention is limited to authenticating a user to the system and authorizing the display of content. It does not deal with attacks on the integrity of subsequent transaction details.
- **WO 2015/014383 A1 Access network selection and connection methods, devices, and computer programs:** This invention deals specifically with granting access to a network. It does not deal with attacks on the integrity of subsequent transaction details.

8.8 Detecting and Defending Against Man-in-the-Middle Attacks

- Crume, J., 2013. *Detecting and Defending Against Man-in-the-Middle Attacks.* USA, Patent No. 8,533,821.
- Crume, J., 2013. *Detecting and Defending Against Man-in-the-Middle Attacks.* USA, Patent No. 8,522,349.

Research Contribution

These US patents provide a means for detecting a large scale MITM attack by monitoring login patterns based upon incoming IP addresses and past user behaviors.

Author's Contribution

Jeff Crume and Jose Bravo collaborated on this patent. Both contributed to this work by developing and refining the idea, documenting the invention, defending the submission before the IBM Invention Disclosure Board, reviewing and providing commentary regarding similar prior art and reviewing the final patent filing.

Differentiation response from 8 January 2007

- **US 7,028,179:** This prior art assumes that a DDoS attack has already been recognized and addresses only mitigation. The present invention deals more with phishing rather than DDoS and provides a means for recognition of the attack.
- **US 7,058,796:** This is like the previous work in that it assumes the attack has already been detected. Further, this invention focuses on wireless LANs rather than phishing.
- **US 2005/0022020:** This requires that the client system be loaded with software, which will communicate with the server to authenticate. The present invention requires no client-side modifications, which is to be expected in phishing attacks.
- **US 2005/0075070:** This deals with wireless networking and depends upon the ability to detect anomalies in the signal based upon intrusion activities. In the case of phishing attacks, no such assumptions can be made with regards to the underlying networking environment since they traverse the global Internet, therefore, the present invention makes no such assumptions.
- **DE10317178A1:** This invention deals specifically with wireless GSM networks and would not be suitable for phishing attacks.
- **Defending Against Redirect Attacks in Mobile IP (Deng, R, et al):** This work deals specifically with IPv6 routing.
- **A Resilient Packet-Forwarding Scheme against Maliciously Packet-Dropping Nodes in Sensor Networks (Lee, S., Choi, Y.):** This deals specifically with routing as well and would require that all nodes in the path participate in the scheme -- an unreasonable requirement in consumer-based phishing defense.
- **Strengthening EPC Tags Against Cloning (Juels, A.):** This deals specifically with and is limited to RFID attacks.
- **Real attacks on virtual networks: Vivaldi out of tune (Kaafar, M., et al):** This is not focused on MITM attacks as the subject is mentioned only in the paper and no formal defense mechanism is outlined.

8.9 Detecting the Presence of Rogue Domain Name Service Providers

- Crume, J., 2015. *System for Detecting the Presence of Rogue Domain Name Service Providers through Passive Monitoring.* USA, Patent No. 9,225,731.
- Crume, J., 2016. *System zum Erfassen des Vorhandenseins eines bösartigen Domain-Name-Service-Providers durch passive Überwachung.* Germany, Patent No. DE 10 2013 208 923 B4.
- Crume, J., 2017. *System for Detecting the Presence of Rogue Domain Name Service Providers through Passive Monitoring.* USA, Patent No. 9,648,033.

Research Contribution

These patents issued in both the US and Germany provide a means for detecting rogue DNS providers, which might, otherwise, misdirect users to an attacker's website rather than the one intended.

Author's Contribution

Jeff Crume was the sole inventor of this work. He developed and refined the idea, documented the invention, defended the submission before the IBM Invention Disclosure Board, reviewed and provided commentary regarding similar prior art and reviewed the final patent filing.

Differentiation response from 22 December 2011

- **Real-Time Detection of Fast Flux Service Networks (Cagalayan, A., et al):** This paper describes a method that narrowly focuses on fast flux DNS switching. The present invention is more general for any sort of DNS spoofing. Also, the technique described here is based upon behavior analysis over time while the present invention makes a determination based a comparison of DNS resolutions to a known, trusted set of addresses.
- **Corrupted DNS Resolution Paths (Dagon, D.):** This presentation is a survey and analysis of certain DNS attacks. It does not describe an invention for preventing them.
- **A Measurement Based Rogue AP Detection Scheme (Han, H., et al):** This paper describes a technique for detecting rogue access points -- not rogue DNS servers. It uses timing differences in network flows (including DNS services) to make its determination but the focus is on APs and no list of known good DNS resolutions is used (which is the basis of the present invention).
- **A Timing-Based Scheme for Rogue AP Detection (Han, H., et al):** This is a publication of the same technique from the same authors described in the previous prior art listing.
- **US 7,756,933 B2 System and Method for Deterring Rogue Users from Attacking Protected Legitimate Servers:** This involves identifying a set of protected users and then creating a set of decoys (called "traps" in the disclosure) to detected attacks. It does not focus on DNS or use a list of known DNS resolutions as the present invention does.
- **US 2006/0176822 A1 Method, System, Service and Computer Program for Identifying Incorrect Domain Name to Internet Protocol (IP) Address Mappings:** This involves a system which actively polls various DNS servers and compares their results looking for errors. The present invention involves passive monitoring, which is more difficult for an attacker to detect.
- **US 2006/0253612 A1 Method and Apparatus for Detecting Responses to Network Queries:** Like the previous invention, this one involves active polling of DNS servers rather than passive monitoring.
- **US 2008/0060054 A1 Method and System for DNS-based Anti-Pharming:** This relies on user input to generate a DNS request which is then sent to multiple DNSs and the results compared. The present invention does not require user input and does not generate DNS requests.
- **US 2009/0327487 A1 Method and System for Discovering DNS Resolvers:** This involves active polling of hosts to determine if they will respond to DNS resolution requests. The present invention involves passive monitoring**.**
- **US 2010/0031362 A1 System and Method for Identification and Blocking of Malicious Use of Servers:** This is imbedded in a network client and involves comparing the currently assigned DNS server to ones used previously by that client and further tests the DNS through active polling and a comparison of the timing of responses from previous DNSs. The present invention typically would reside outside of a client and does not generate DNS requests as this one does.
- **US 2010/0262688 A1 Systems, Methods, and Devices for Detecting Security Vulnerabilities in IP Networks:** This invention utilizes a fingerprinting technique to compare whether hosts have been tampered with along with some active polling techniques.
- **US 2010/0291943 A1 Method and Apparatus for Pooling Network Resources:** This invention involves a technique for pooling network resources. It is not focused on detecting rogue DNS servers.

- **US 2011/0106919 A1 Automated DNS Configuration with Local DNS Server:** This invention involves a technique for automating DNS configuration using a DHCP server. It is not focused on detecting rogue DNS servers.
- **US 2011/0191455 A1 Using Aggregated DNS Information Originating from Multiple Sources to Detect Anomalous DNS Name Resolutions:** This invention is similar to others described above where results from various DNS servers are compared in order to identify discrepancies. It does not use a list of known resolutions as the present invention does.
- **US 2011/0231931 A1 Method and Device for Preventing Domain Name System Spoofing:** This involves active polling of DNS servers while the present uses passive monitoring.

8.10 Migration Across Authentication Systems

- Crume, J., 2010. *Migration Across Authentication Systems.* USA, Patent No. US2010/0269151A1.

Research Contribution

This US patent filing provides a means for nondisruptive migration of users from one authentication system to another.

Author's Contribution

Jeff Crume was the sole inventor of this work. He developed and refined the idea, documented the invention, defended the submission before the IBM Invention Disclosure Board, reviewed and provided commentary regarding similar prior art and reviewed the final patent filing.

Differentiation response from 3 Dec 2008

- **Adaptive Resource Sharing in a Web Services Environment (Naik, V.):** This paper describes a middleware architecture that deals with sharing resources based upon workloads and doesn't appear to have anything to do with security.
- **US 7,185,359 B2 Authentication and Authorization Across Autonomous Network Systems:** This patent deals with how to trust the authentication done on a different system -- not how to migrate userids.
- **Harmony: A Desktop Grid for Delivering Enterprise Computations (Naik, V.):** This paper describes a grid infrastructure designed to deal with user privacy and responsiveness and is not applicable to migrating userids.
- **US 2008/0109448 A1 System and Method for Managing Data Across Multiple Environments:** This deals with data management across various systems. The portion that deals with authentication is focused exclusively on eliminating the need for the user to keep track of multiple userids but does not deal with migrating userids.
- **US 2008/0046434 A1 Centralized Management of Technical Records Across an Enterprise:** This invention deals with controlling access to records across multiple system rather than migrating userids.
- **US 2008/0028205 A1 Method and Apparatus for Authenticating a User:** This deals with using multimedia data as a means to authenticate a user -- not migrating userids.
- **US 2007/0083917 A1 Apparatus System and Method for Real-Time Migration of Data Related to Authentication:** The present invention has some novel features that this invention does not include. One is the presence of an optional migration file which lists which users are to be migrated. This allows for far more control over the migration process by providing a means for a phased migration. This way the

organization can choose to migrate any sized subset of the user base which avoids two very important risks: 1) if there is a failure in the migration process, the impact is minimized to a chosen set of users and 2) the additional processing overhead of the migration process can be spread out over time rather than incurred all at once when all users log in (say, first thing on a Monday morning). In addition, the present invention explicitly deals with the migration of the password expiry interval which: 1) saves users from having to create a new password during the migration process (effectively having to log in twice) and 2) avoids the potential of an unintended lengthening of the password expiry (since the new system would see the password as being new and, therefore, resetting the expiry clock).

- **At the Forge (Lerner, R.):** This article deals with authentication using the OpenID standard and not migrating userids.

8.11 Mobile Device Reset

- Bravo, J., Crume, J. & Hinds, N., 2015. *Mobile Device Reset.* USA, Patent No. 9,078,135.
- Bravo, J., Crume, J. & Hinds, N., 2015. *Mobile Device Password Reset.* USA, Patent No. 9,088,896.

Research Contribution

These US patents provide a means for securely regaining control of a mobile device for which the password has been lost. Given the increasing importance of mobile devices as an authenticator, such a capability is important in supporting the authentication system.

Author's Contribution

Jeff Crume, Nigel Hinds and Jose Bravo collaborated on this patent. Both contributed to this work by developing and refining the idea, documenting the invention, defending the submission before the IBM Invention Disclosure Board, reviewing and providing commentary regarding similar prior art and reviewing the final patent filing.

Differentiation response from 21 June 2013

- **IPCOM000224591D Automatic Mobile Phone Unlock Beyond a Predetermined Call Duration Threshold of a Trusted Call:** This is a convenience mechanism for the case when the user is being called from a known/trusted phone number, however, as an access recovery mechanism it does not address the possibility where caller-ID has been compromised. Further, the user is not required to set a new passcode. The present invention, however, extends this notion to a more secure means of recovering a mobile device with a lost passcode. For example, the mobile device will disconnect the call originated by the trusted phone and call back with a random one-time PIN. The PIN must be entered on the mobile device within a predetermined period. Once the mobile device is unlocked the user is forced into a passcode reset process. This mechanism can also be combined with a lock-out mechanism, so after a certain number of failed logins, the device can only be unlocked using the disclosed method.
- **US20110159844A1 Method and apparatus for user interaction while device is locked:** This is another convenience mechanism to allow access to an otherwise locked mobile device. It includes methods to authenticate the current device user to the device owner, who is remote, or a third party. This invention initiates the process from the mobile device and requires another party to grant access. In the present invention the owner authenticates him/herself to the mobile device by using a second phone to which only the owner has physical access (trusted phone number).

9 APPENDIX – PRIOR PUBLICATIONS

9.1 WEBSITE AUTHENTICATION


US008762724B2

(12) **United States Patent**
Bravo et al.

(10) **Patent No.: US 8,762,724 B2**
(45) **Date of Patent: Jun. 24, 2014**

(54) **WEBSITE AUTHENTICATION**

(75) Inventors: **Jose Bravo**, Mamaroneck, NY (US); **Jeffrey L. Crume**, Raleigh, NC (US)

(73) Assignee: **International Business Machines Corporation**, Armonk, NY (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **13/613,502**

(22) Filed: **Sep. 13, 2012**

(65) **Prior Publication Data**

US 2013/0007859 A1 Jan. 3, 2013

Related U.S. Application Data

(63) Continuation of application No. 12/423,928, filed on Apr. 15, 2009.

(51) **Int. Cl.**
H04L 29/06 (2006.01)

(52) **U.S. Cl.**
USPC **713/169**; 713/168; 713/170; 713/171; 713/172; 713/150; 726/2; 726/3; 726/4; 726/26; 726/27; 380/278; 380/282; 380/283

(58) **Field of Classification Search**
None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,310,720	A	1/1982	Check, Jr.
5,046,082	A	9/1991	Zicker et al.
5,068,894	A	11/1991	Hoppe
5,323,465	A	6/1994	Avarne
5,457,737	A	10/1995	Wen
5,491,752	A	2/1996	Kaufman et al.
5,497,411	A	3/1996	Pellerin
5,647,388	A	7/1997	Butler, Jr. et al.
5,657,388	A	8/1997	Weiss
5,684,950	A	11/1997	Dare et al.
5,701,339	A	12/1997	Suda
5,749,052	A	5/1998	Hidem et al.
5,841,871	A	11/1998	Pinkas
5,842,124	A	11/1998	Kenagy et al.
5,892,902	A	4/1999	Clark
5,953,422	A	9/1999	Angelo et al.
5,971,272	A	10/1999	Hsiao
6,000,031	A	12/1999	Bingaman et al.
6,169,890	B1	1/2001	Vatanen
6,278,863	B1	8/2001	Mabrouki

(Continued)

FOREIGN PATENT DOCUMENTS

DE	10317176	A1	11/2004
EP	1119147	A1	7/2001

(Continued)

OTHER PUBLICATIONS

Zia, Notice of Allowance and Fee(s) Due for U.S. Appl. No. 12/423,928 dated Dec. 4, 2012, 19 pages.

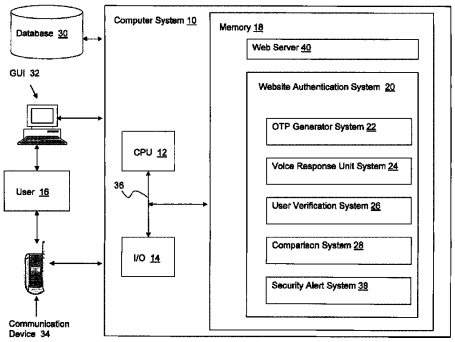
(Continued)

Primary Examiner — Michael R Vaughan
(74) *Attorney, Agent, or Firm* — Douglas A. Lashmit; Hoffman Warnick LLC

(57) **ABSTRACT**

Embodiments of website authentication including receiving a request from a user to view a website within a graphical user interface (GUI); generating a one time password (OTP); storing the generated OTP in a database; displaying the generated OTP on the GUI; verifying an identity of the user by receiving an identification datum from a communication device; receiving an entered OTP from the user; comparing the entered OTP with the generated OTP; and communicating whether the website is authenticated.

10 Claims, 2 Drawing Sheets



(56) **References Cited**

U.S. PATENT DOCUMENTS

6,308,268 B1 10/2001 Audebert
6,324,271 B1 11/2001 Sawyer et al.
6,330,608 B1 12/2001 Stiles
6,334,056 B1 12/2001 Holmes et al.
6,338,140 B1 1/2002 Owens et al.
6,349,134 B1 2/2002 Katz
6,385,729 B1 5/2002 DiGiorgio et al.
6,387,729 B2 5/2002 Eng et al.
6,393,468 B1 5/2002 McGee
6,400,726 B1 6/2002 Piret et al.
6,466,780 B1 10/2002 Geiselman et al.
6,535,726 B1 3/2003 Johnson
6,584,309 B1 6/2003 Whigham
6,687,241 B1 2/2004 Goss
6,707,915 B1 3/2004 Jobst et al.
6,731,731 B1 5/2004 Ueshima
6,993,658 B1 1/2006 Engberg et al.
6,993,663 B1 1/2006 Paya et al.
7,007,301 B2 2/2006 Crosbie et al.
7,024,688 B1 4/2006 Faccin et al.
7,028,179 B2 4/2006 Anderson et al.
7,058,796 B2 6/2006 Lynn et al.
7,058,968 B2 6/2006 Rowland et al.
7,100,204 B1 8/2006 Myllymaki et al.
7,133,662 B2 11/2006 Bravo et al.
7,142,840 B1 11/2006 Geddes et al.
7,221,949 B2 5/2007 Clough
7,290,278 B2 10/2007 Cahill et al.
7,317,693 B1 1/2008 Roesch et al.
7,324,976 B2 1/2008 Gupta et al.
7,337,431 B1 2/2008 Barnes et al.
7,357,310 B2 4/2008 Calabrese et al.
7,360,248 B1 4/2008 Kanevsky et al.
7,376,431 B2 5/2008 Niedermeyer
7,379,921 B1 5/2008 Kiliccote
7,380,708 B1 6/2008 Kiliccote
7,447,494 B2 11/2008 Law et al.
7,480,805 B1 1/2009 Gnech et al.
7,491,308 B2 2/2009 Talieh et al.
7,519,989 B2 4/2009 Lin et al.
7,533,414 B1 5/2009 Reed et al.
7,536,634 B2 5/2009 Green et al.
7,540,022 B2 5/2009 Barari et al.
7,594,270 B2 9/2009 Church et al.
7,600,676 B1 10/2009 Rados et al.
7,609,625 B2 10/2009 Wei et al.
7,623,458 B2 11/2009 Ayyagari et al.
7,624,447 B1 11/2009 Horowitz et al.
7,665,128 B2 2/2010 Yang
7,673,334 B2 3/2010 Takemori et al.
7,715,823 B2 5/2010 Bravo et al.
7,716,742 B1 5/2010 Roesch et al.
7,757,285 B2 7/2010 Kubota
7,765,584 B2 7/2010 Roskind
7,779,465 B2 8/2010 Baker et al.
7,823,199 B1 10/2010 Rathi et al.
7,840,993 B2 11/2010 Ganesan et al.
7,845,004 B2 11/2010 Bardsley et al.
7,886,346 B2 2/2011 Sandhu et al.
7,926,108 B2 4/2011 Rand et al.
7,954,150 B2 5/2011 Croft et al.
7,975,293 B2 7/2011 Yoshida et al.
8,019,995 B2 9/2011 van Bemmel
8,024,567 B2 9/2011 Han
8,050,658 B2 11/2011 Hong
8,060,915 B2 11/2011 Voice et al.
8,136,150 B2 3/2012 Hayler et al.
8,150,370 B2 4/2012 Dempo et al.
8,151,327 B2 4/2012 Eisen
8,181,248 B2 5/2012 Oh et al.
8,201,217 B1 6/2012 Begen et al.
8,254,542 B2 8/2012 Frederick
8,281,375 B2 10/2012 von Krogh
8,285,639 B2 10/2012 Eden et al.
8,296,823 B2 10/2012 Schubert
8,301,877 B2 10/2012 Grajek et al.
8,302,180 B1 10/2012 Gudov et al.
8,302,187 B1 10/2012 Gupta et al.
2001/0054155 A1 12/2001 Hagan et al.
2002/0069165 A1 6/2002 O'Neil et al.
2002/0091931 A1 7/2002 Quick et al.
2002/0095588 A1 7/2002 Shigematsu et al.
2002/0178070 A1 11/2002 Leveridge
2002/0178370 A1 11/2002 Gurevich et al.
2003/0014315 A1 1/2003 Jaalinoja et al.
2003/0154382 A1 8/2003 Vicard
2003/0172272 A1 9/2003 Ehlers et al.
2004/0148520 A1 7/2004 Talpade et al.
2004/0152446 A1 8/2004 Saunders et al.
2004/0198329 A1 10/2004 Vasa
2004/0243856 A1 12/2004 Shatford
2005/0015624 A1 1/2005 Ginter et al.
2005/0018618 A1 1/2005 Mualem et al.
2005/0022020 A1 1/2005 Fremberg
2005/0060535 A1 3/2005 Bartas
2005/0075070 A1 4/2005 Crilly, Jr.
2005/0182958 A1 8/2005 Pham et al.
2005/0187934 A1 8/2005 Motsinger et al.
2005/0188423 A1 8/2005 Motsinger et al.
2005/0210251 A1 9/2005 Nyberg et al.
2006/0021031 A1 1/2006 Leahy et al.
2006/0036690 A1 2/2006 O'Neil
2006/0094403 A1 5/2006 Norefors et al.
2006/0095955 A1 5/2006 Vong
2006/0179304 A1 8/2006 Han
2006/0248021 A1 11/2006 Jain et al.
2006/0288411 A1 12/2006 Garg et al.
2007/0015492 A1 1/2007 Bravo et al.
2007/0067828 A1 3/2007 Bychkov
2007/0083606 A1 4/2007 Malik et al.
2007/0084913 A1 4/2007 Weston
2007/0107050 A1 5/2007 Selvarajan
2007/0136573 A1 6/2007 Steinberg
2007/0136808 A1 6/2007 Xiong
2007/0143851 A1 6/2007 Nicodemus et al.
2007/0186099 A1 8/2007 Beck et al.
2007/0220275 A1 9/2007 Heitzeberg et al.
2007/0234426 A1 10/2007 Khanolkar et al.
2007/0261112 A1 11/2007 Todd et al.
2007/0266257 A1 11/2007 Camaisa et al.
2008/0028447 A1 1/2008 O'Malley et al.
2008/0172730 A1 7/2008 Sandhu et al.
2008/0181380 A1 7/2008 Gustave et al.
2008/0189776 A1 8/2008 Constable
2008/0209275 A1 8/2008 Kwan et al.
2008/0270301 A1 10/2008 Jones et al.
2008/0281737 A1 11/2008 Fajardo
2008/0318548 A1 12/2008 Bravo et al.
2009/0037329 A1 2/2009 Coppinger et al.
2009/0077637 A1 3/2009 Santos et al.
2009/0094682 A1 4/2009 Sage et al.
2009/0095588 A1 4/2009 Thomas
2009/0104889 A1 4/2009 Lotvonen et al.
2009/0106138 A1 4/2009 Smith et al.
2009/0300738 A1 12/2009 Dewe et al.
2010/0024017 A1 1/2010 Ashfield et al.
2010/0051686 A1 3/2010 Obi
2010/0095351 A1 4/2010 Liu et al.
2010/0269162 A1 10/2010 Bravo et al.
2011/0015449 A1 1/2011 Pendleton et al.
2011/0039237 A1 2/2011 Skare
2011/0138483 A1 6/2011 Bravo et al.
2011/0197070 A1 8/2011 Mizrah
2011/0225647 A1 9/2011 Dilley et al.
2011/0277024 A1 11/2011 Begley et al.
2011/0289576 A1 11/2011 Cheng
2011/0307366 A1 12/2011 Ahuja et al.
2012/0011066 A1 1/2012 Telle et al.
2012/0149334 A1 6/2012 Zhang et al.
2012/0204241 A1 8/2012 Varsavsky Waisman-Diamond et al.
2012/0264405 A1 10/2012 Bravo
2012/0272331 A1 10/2012 Lemaster et al.
2013/0007859 A1 1/2013 Bravo et al.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2014/0011561	A1	1/2014	Lutnick et al.
2014/0016634	A1	1/2014	Khan et al.
2014/0033279	A1	1/2014	Nimashakavi et al.

FOREIGN PATENT DOCUMENTS

GB	2456509	A	7/2009
JP	10334048		12/1998
JP	10341224		12/1998
JP	20011111545		4/2001
WO	0109808	A1	8/2001
WO	2004079499	A2	9/2004
WO	2006103387	A1	10/2006
WO	2008147353	A1	12/2008

OTHER PUBLICATIONS

Ma et al., "Beyond Blacklists: Learning to Detect Malicious Web Sites from Suspicious URLs", KDD '09, Jul. 28-Jul. 1, 2009, pp. 1245-1253.

Lakhia, U.S. Appl. No. 13/432,956, Notice of Allowance & Fees Due, Apr. 15, 2013, 27 pages.

Bibbee, U.S. Appl. No. 11/765,193, Examiner's Answer, Apr. 16, 2013, 20 pages.

Almeida, U.S. Appl. No. 12/630,875, Office Action, Apr. 17, 2013, 40 pages.

Lakhia, U.S. Appl. No. 11/753,673, Notice of Allowance & Fees Due, dated May 10, 2013, 28 pages.

Kumaraguru et al., "Getting Users to Pay Attention to Anti-Phishing Education: Evaluation of Retention and Transfer", APWG eCrime Researchers Summit, Oct. 4-5, 2007, pp. 70-81, Pittsburgh, PA.

Ben Adida, "Beamauth: Two-Factor Web Authentication With a Bookmark"; CCS, Oct. 29-Nov. 2, 2007, pp. 48-57, Alexandria, VA.

Nassar et al., "Holistic VoIP Instrusion Detection and Prevention System", IPTCOMM, 2007, pp. 1-9, New York.

Stoll et al., "Sesame: Informing User Security Decisions With System Visualization", CHI, Apr. 5-10, 2008, pp. 1045-1054, Florence Italy.

Sharief Abdel Megeed, USPTO Office Action, U.S. Appl. No. 12/423,928, Notification Date Aug. 25, 2011, 21 pages.

Sharief Abdel Megeed, USPTO Final Office Action, U.S. Appl. No. 12/423,928, Notification Date Nov. 10, 2011, 20 pages.

Syed Zia, USPTO Office Action, U.S. Appl. No. 12/423,928, Notification Date Jun. 8, 2012, 20 pages.

Syed Zia, USPTO Notice of Allowance and Fee(s) Due, U.S. Appl. No. 12/423,928, Date Mailed Sep. 25, 2012, 10 pages.

Lakhia, Office Action Communication for U.S. Appl. No. 11/753,673 dated Oct. 8, 2010, 13 pages.

Lakhia, Office Action Communication for U.S. Appl. No. 11/753,673 dated Apr. 15, 2010, 13 pages.

Lakhia, Office Action Communication for U.S. Appl. No. 11/753,673 dated Dec. 22, 2011, 15 pages.

Lakhia, Notice of Allowance and Fee(s) Due for U.S. Appl. No. 11/753,673 dated Jun. 18, 2012, 11 pages.

Bibbee, Office Action Communication for U.S. Appl. No. 11/765,193 dated Apr. 16, 2012, 18 pages.

Bibbee, Office Action Communication for U.S. Appl. No. 11/765,193 dated Sep. 19, 2011, 18 pages.

Bibbee, Office Action Communication for U.S. Appl. No. 11/765,193 dated May 21, 2011, 17 pages.

Bibbee, Office Action Communication for U.S. Appl. No. 11/765,193 dated Nov. 29, 2010, 14 pages.

Bibbee, Office Action Communication for U.S. Appl. No. 11/765,193 dated Jul. 30, 2010, 15 pages.

Bibbee, Office Action Communication for U.S. Appl. No. 11/765,193 dated Feb. 18, 2010, 15 pages.

Geneiatakis et al., "Survey of Security Vulnerabilities in Session Initiation Protocol," 2006, pp. 68-81, IEEE Communications Surveys, vol. 8, No. 3.

Deng et al., "Defending Against Redirect Attacks in Mobile IP," Nov. 2002, pp. 59-67, CCS 2002.

Juels, "Strengthening EPC Tags Against Cloning," Sep. 2005, pp. 67-75, WiSE 2005.

Kaafar et al., "Real attacks on virtual networks: Vivaldi out of tune," Sep. 2006, pp. 139-146, SIGCOMM 2006 Workshops.

Lee et al., "A Resilient Packet-Forwarding Scheme Against Maliciously Packet-Dropping Nodes in Sensor Networks," Oct. 2006, pp. 59-69, SASN 2006.

Lakhia, U.S. Appl. No. 11/753,673, Notice of Allowance, Aug. 21, 2012, 7 pages.

Tran, U.S. Appl. No. 11/524,340, Notice of Allowance, Dec. 29, 2009, 11 pages.

Tran, U.S. Appl. No. 11/524,340, Office Action, Jul. 29, 2009, 9 pages.

Tran, U.S. Appl. No. 11/524,340, Office Action, Oct. 31, 2008, 19 pages.

Tran, U.S. Appl. No. 11/524,340, Office Action, May 27, 2008, 22 pages.

Tran, U.S. Appl. No. 11/524,340, Office Action, Apr. 29, 2009, 7 pages.

Lakhia, U.S. Appl. No. 11/753,673, Notice of Allowance, Jan. 8, 2013, 14 pages.

"Prevent Online Banking Fraud", Dec. 7, 2010, http://www.phonefactor.com/products/transaction-verification, 1 page.

Bonzo, U.S. Appl. No. 11/776,619, Office Action, Sep. 30, 2009, 12 pages.

Bonzo, U.S. Appl. No. 11/776,619, Notice of Allowance, Apr. 29, 2010, 10 pages.

Alicherry et al., Double Check: Multi-path Verification Against Man-in-the-Middle Attacks, 2009 IEEE, pp. 557-563.

Koo et al., "VoIP Interception in P2P SIP Environment", 2010 IEEE, vol. 1, pp. 331-334.

Kopsidas et al., "Voice Interactive Personalized Security (VoIPSEC) protocol: Fortify Internet telephony by providing end-to-end security through inbound key exchange and biometric verification", 1-4244-0595-5 /06/$20.00 © 2006 IEEE, 10 pgs.

Leung, "Depress Phishing by CAPTCHA with OTP", The Chinese University of Hong Kong, 2009, ASID, Aug. 20-22, 2009, 6 pgs.

Nassar et al., Holistic VoIP Intrusion Detection and Prevention System, IPTCOMM '07, ACM 2007, 9 pgs.

Almeida, U.S. Appl. No. 12/630,875, Office Action, Mar. 1, 2012, 17 pages.

Almeida, U.S. Appl. No. 12/630,875, Office Action, Aug. 30, 2012, 14 pages.

Almeida, U.S. Appl. No. 12/630,875, Notice of Allowance, Dec. 20, 2012, 7 pages.

Lakhia, U.S. Appl. No. 13/432,956, Office Action, Feb. 14, 2013, 26 pages.

Gee, U.S. Appl. No. 13/084,823, Office Action, Mar. 11, 2013, 8 pages.

Gee, U.S. Appl. No. 13/084,823, Office Action Communication, Jul. 19, 2013, 24 pages.

Almeida, U.S. Appl. No. 12/630,875, Office Action Communication, Aug. 7, 2013, 15 pages.

U.S. Appl. No. 12/630,875, Notice of allowance and Fee(s) Due dated Nov. 18, 2013, IBMC-0353, 19 pages.

Vaughan, U.S. Appl. No. 12/423,928, Notice of Allowance & Fees Due, Jul. 11, 2013, 25 pages.

U.S. Appl. No. 13/084,826, Office Action dated Feb. 3, 2014, IBMC-0395, 12 pages.

U.S. Appl. No. 13/562,491, Office Action dated May 5, 2014, 64 pages.

U.S. Appl. No. 13/084,823, Notice of Allowance and Fees Due, May 1, 2014, 16 pages.

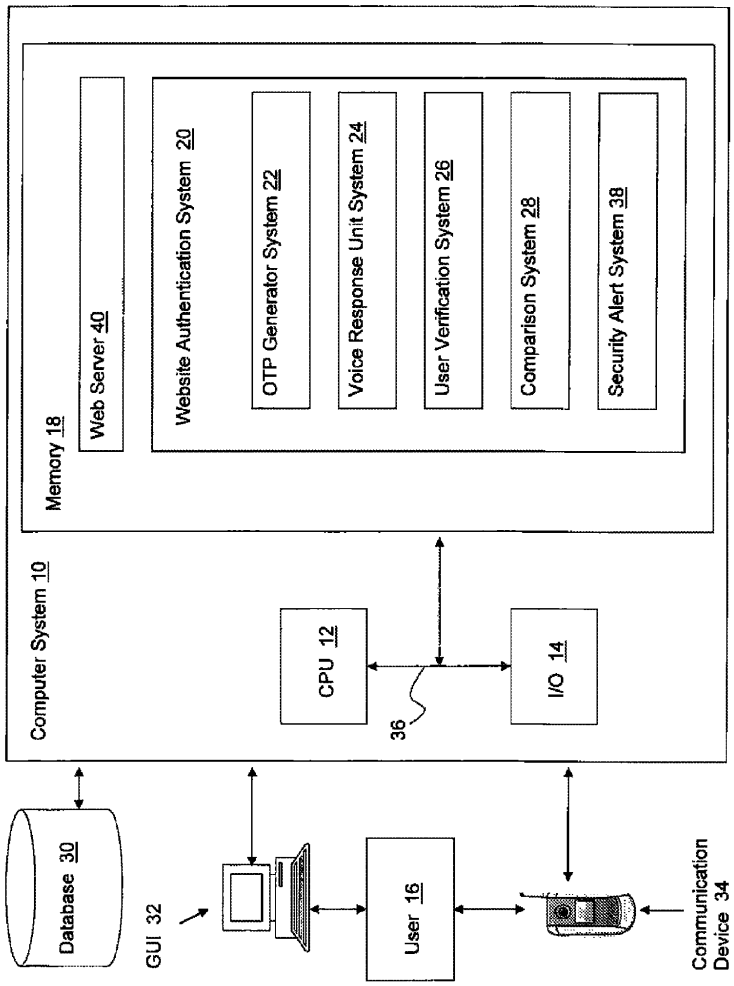

Computer System 10
Memory 18
Web Server 40
Website Authentication System 20
OTP Generator System 22
Voice Response Unit System 24
User Verification System 26
Comparison System 28
Security Alert System 38
CPU 12
I/O 14
36
Database 30
GUI 32
User 16
Communication Device 34

FIG. 1

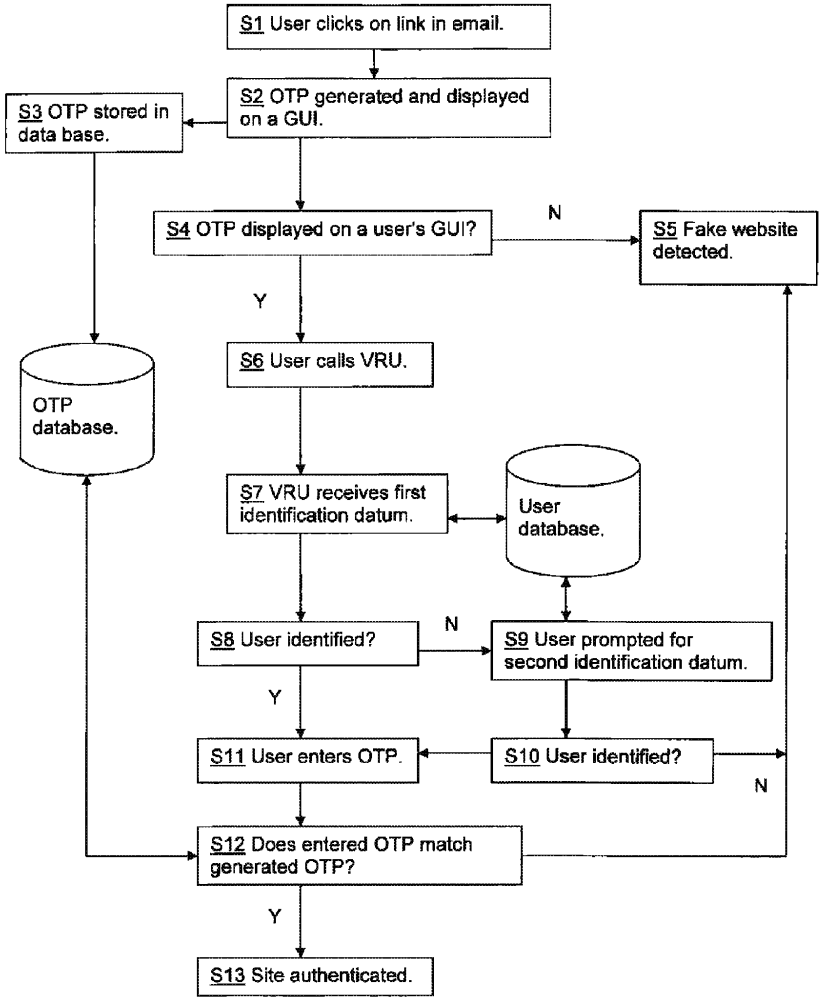

S1 User clicks on link in email.
S2 OTP generated and displayed on a GUI.
S3 OTP stored in data base.
S4 OTP displayed on a user's GUI?
N
S5 Fake website detected.
Y
S6 User calls VRU.
OTP database.
S7 VRU receives first identification datum.
User database.
S8 User identified?
N
S9 User prompted for second identification datum.
Y
S11 User enters OTP.
S10 User identified?
N
S12 Does entered OTP match generated OTP?
Y
S13 Site authenticated.

FIG. 2

WEBSITE AUTHENTICATION

This application is a continuation application of co-pending U.S. patent application Ser. No. 12/423,928, filed on Apr. 15, 2009, which is hereby incorporated herein.

FIELD OF THE INVENTION

The present invention relates generally to website authentication, and more particularly to website authentication using a one time password and a voice response unit.

BACKGROUND OF THE INVENTION

Computers and other devices, as well as secure facilities, services and financial accounts, often contain proprietary, personal and/or sensitive information, which could be compromised if accessed by unauthorized individuals. Thus such devices, facilities, services and accounts (hereinafter "restricted items") often incorporate security techniques, such as database access control mechanisms, to prevent unauthorized users from accessing, obtaining, or altering the proprietary, personal and/or sensitive information. Authentication techniques allow users to prove their identity and obtain authorized access to a given restricted item.

In a phishing attack, a user is tricked into providing login credentials and/or sensitive information by an attacker impersonating an authentic website. The reason the attack succeeds is that the user is unable to determine whether the website is authentic or fake. Most existing defenses require the user to discern an authentic from fake website based upon the overall appearance of the website, a specially chosen website authentication image, or verification of the website's digital certification. Appearances may be imitated by the attacker or overlooked by the user.

Website authentication, either in addition to or as an alternative to appearance based defenses against phishing attacks, improves security for both users and the entities that utilize websites in communicating with users.

SUMMARY OF THE INVENTION

The present invention provides a method, system and program product to improve website authentication. In particular, the present invention allows users to authenticate the website that they are visiting.

In a first aspect, the invention provides a method for website authentication, using at least one computer hardware device for performing the steps of: receiving a request from a user to view a website within a graphical user interface (GUI); generating a one time password (OTP); storing the generated OTP in a database; displaying the generated OTP on the GUI; verifying an identity of the user by receiving an identification datum from a communication device; receiving an entered OTP from the user; comparing the entered OTP with the generated OTP; and communicating whether the website is authenticated.

In a second aspect, the invention provides a website authentication system, including a computer hardware device comprising: a one time password (OTP) generator system for generating a OTP; a voice response unit (VRU) system for receiving at least one identification datum from a communication device; a user verification system for verifying an identity of the user by receiving an identification datum from the communication device; a comparison system for receiving an entered OTP from the user and comparing the entered OTP with the generated OTP; and a security alert system for communicating whether the website is authenticated.

In a third aspect, the invention provides a computer readable medium storing a program product for website authentication, comprising: program code for receiving a request from a user to view a website within a graphical user interface (GUI); program code for generating a one time password (OTP); program code for storing the generated OTP in a database; program code for displaying the generated OTP on the GUI; program code for verifying an identity of the user by receiving an identification datum from a communication device; program code for receiving an entered OTP from the user; program code for comparing the entered OTP with the generated OTP; and program code for communicating whether the website is authenticated.

BRIEF DESCRIPTION OF THE DRAWINGS

The above and other objects, features and advantages of the invention will be better understood by reading the following more particular description of the invention in conjunction with the accompanying drawings.

FIG. **1** depicts one embodiment of a website authentication system in accordance with this invention.

FIG. **2** is a flow chart of one embodiment of the main steps for website authentication in accordance with this invention.

The drawings are not necessarily to scale. The drawings are merely schematic representations, not intended to portray specific parameters of the invention. The drawings are intended to depict only typical embodiments of the invention, and therefore should not be considered as limiting the scope of the invention. In the drawings, like numbering represents like elements.

DETAILED DESCRIPTION OF THE INVENTION

FIG. **1** shows an illustrative embodiment of the invention in which a computer system **10** having a web server **40** provides web pages to a user **16** via a graphical user interface (GUI) **32**. In addition to web server **40**, a website authentication system **20** is also provided to allow user **16** to authenticate content allegedly being served from web server **40**. Website authentication system **20**, as well as web server **40**, may be implemented as a software program product that can be stored in memory **18** and be executed on any type of computer system **10**. A person skilled in the art will recognize that the invention may be implemented on one or more computer systems and this disclosure is not intended to limit such potential embodiments. In this illustrative embodiment, website authentication system **20** includes a one time password (OTP) generator system **22**; a voice response unit (VRU) system **24**; a user verification system **26**; a comparison system **28**; and a security alert system **38**.

In operation, website authentication system **20** receives a request from the user **16** to view a website on the GUI **32**. An input/output (I/O) system **14** is provided on the computer system **10** for communications with the user **16** via GUI **32** and/or a communication device **34**. Communication device **34** may be implemented using any type of communication device including, for example, a telephone, a cell phone, a personal digital assistant (PDA) and a radio. GUI **32** may be implemented using any type of device or software that permits website access including, for example, a browser, a desktop computer, a laptop computer, a PDA, a cell phone. GUI **32** and communication device **34** may reside on different devices or the same device.

OTP generator system **22** generates a one time password (OTP) when the user **16** attempts to view the website. The generated OTP may include at least one number, letter, and other symbol. In one embodiment of the invention, the generated OTP is limited to numeric digits for easy phone keypad entry. The generated OTP is stored in a database **30** and displayed on the GUI **32**.

Once displayed, user **16** reads the generated OTP from the GUI **32** which can then be used to authenticate the website via the communication device **34**. As used herein "reads" means accesses the generated OTP by visual, audio, tactile or any other communication method between GUI **32** and user **16**.

At some point after the OTP is generated, voice response unit system (VRU) **24** receives a communication, e.g., a telephone call, from user **16** by communication device **34**. In one embodiment, a VRU phone number is previously communicated to user **16** through a communication channel other than the website thereby preventing the phishing attack from posting a fake VRU phone number. VRU **24** may receive an identification datum from the communication device **34**. The identification datum may include an identification datum automatically generated by the communication device or an identification datum input by the user **16**. The identification datum may include a caller ID, an account number, a password or a first geographical location. VRU may prompt user **16** to enter identification datum over the communication device **34**, e.g., via a key pad, by speaking, etc.

User verification system **26** can verify an identity of the user **16** in a number of ways. In one approach, user verification system **26** may verify the user **16** by comparing at least one identification datum with a previously stored identification datum in the database. User verification system **26** may determine a second geographical location by detecting the location of the GUI **32** where the request from the user to view the website was made and then store the second geographical location in the database **30**. In another approach, user verification system **26** may verify the user **16** by comparing the first geographical location with the second geographical location. If user's **16** identity cannot be verified, user verification system **26** notifies voice response unit **24** to terminate the communication and notifies the security alert system **38** of a failed user verification attempt.

If user's **16** identity is verified, user **16** enters the OTP that user reads from the GUI **32**. Comparison system **28** receives the entered OTP from the user **16**. Comparison system **28** compares the entered OTP with the generated OTP in the database **30**.

If the entered OTP matches the generated OTP, then website authentication system **20** communicates to the user **16** that the website being viewed by the user **16** is authentic. If the entered OTP does not match the generated OTP, then website authentication system **20** communicates to the user **16** via the communication device **34** that the website being viewed by the user is fake. In one embodiment, if the entered OTP does not match the generated OTP, comparison system notifies the security alert system **38** that a fake website has been detected.

In one embodiment if a fake website is detected, security alert system **38** may store the fake website in the database **30**. Storing the fake website may include storing information about the fake website including the website address of the fake website and html coding of the fake website. Security alert system **38** may notify an authentic website administrator of the report of the fake website.

Referring now to FIG. **2**, one embodiment of the process of website authentication as defined by the present invention is described. The process starts at S**1** when user **16** clicks on a link in an email. Email is a common method for disseminating fake websites for purposes of deceiving users **16** into conveying proprietary, personal and/or secure information. Clicking a link in an email is illustrative, the teachings of the invention apply to any means of a user **16** accessing a website.

After the website is accessed, at S**2** an OTP is generated and displayed on a GUI **32**. Both an authentic website and a fake website could generate an OTP and display the OTP on a GUI **32**. At S**3** the generated OTP is stored in a database **30**. If at S**4** an OTP is not displayed on a user's GUI **32** then at S**5** a fake website has been detected by the user **16**. If at S**4** an OTP is displayed, then at S**6** user **16** telephones the VRU **24**.

At S**7** VRU **24** receives a first identification datum. First identification datum may be an identification datum automatically generated by the communication device **34**. At S**8**, user identity is verified by comparing the first identification datum with known information in the database **30**. If at S**8** the user **16** is identified, then at S**11** the user **16** will enter the OTP displayed on the GUI **32**. If at S**8** the user **16** is not identified, then at S**9** the user **16** may be prompted for the second identification datum. Second identification datum may include, for example, an account number, a password, a personal identification number, date of birth, Social Security number or any number of identification data that would be previously stored in the database **30**. If at S**10** the second identification datum matches information in the user database, then user is identified. If at S**10** the second identification datum does not match information in the user database, then user **16** is not identified. Second identification datum may include the first geographical location from where the call is being initiated. The second geographical location from the GUI **32** where the website was accessed may be detected and stored in the database **30**. If at S**10** the first geographical location matches the second geographical location, then user **16** is identified. If at S**10** the first geographical location does not match the second geographical location, then user **16** is not identified. A person skilled in the art will readily recognize that any number of methods for verifying the identity of the user **16** may be used. A person skilled in the art will also recognize that the number of steps of verifying user identity could be added or subtracted depending upon the level of security desired.

At S**11**, after user **16** is identified, user **16** enters the OTP that is displayed on the website being accessed. The entered OTP is compared with the generated OTP in the database S**12**. If the entered OTP matches the generated OTP then the website is authenticated S**13**. If the entered OTP does not match the generated OTP then a fake website is detected S**5**.

Referring again to FIG. **1**, a person skilled in the art will readily recognize that in the event of website authentication any number of communications could be generated to the user through the website on the GUI **32** or communication device **34**. In the event of a fake website being detected, any type of communication or warning could be generated to the user on the communication device **34** (as the website being viewed by the user **16** would be a fake website). Once the user **16** received such a communication, the user **16** could immediately terminate interaction with the website.

I/O **14** may comprise any system for exchanging information to/from an external resource. External devices/resources may comprise any known type of external device, including a monitor/display, speakers, storage, another computer system, a hand-held device, keyboard, mouse, voice recognition system, speech output system, printer, facsimile, pager, etc. Bus **36** provides a communication link between each of the components in the computer system **10** and likewise may comprise any known type of transmission link, including electrical, optical, wireless, etc. Although not shown, additional

components, such as cache memory, communication systems, system software, etc., may be incorporated into computer system **10**.

Access to computer system **10** may be provided over a network such as the Internet, a local area network (LAN), a wide area network (WAN), a virtual private network (VPN), etc. Communication could occur via a direct hardwired connection (e.g., serial port), or via an addressable connection that may utilize any combination of wireline and/or wireless transmission methods. Moreover, conventional network connectivity, such as Token Ring, Ethernet, WiFi or other conventional communications standards could be used. Still yet, connectivity could be provided by conventional TCP/IP sockets-based protocol. In this instance, an Internet service provider could be used to establish interconnectivity. Further, as indicated above, communication could occur in a client-server or server-server environment.

It should be appreciated that the teachings of the present invention could be offered as a business method on a subscription or fee basis. For example, a computer system **10** comprising a website authentication system **20** could be created, maintained and/or deployed by a service provider that offers the functions described herein for customers.

It is understood that in addition to being implemented as a system and method, the features may be provided as a program product stored on a computer-readable medium, which when executed, enables computer system **10** to provide a website authentication system **20**. To this extent, the computer-readable medium may include program code, which implements the processes and systems described herein. It is understood that the term "computer-readable medium" comprises one or more of any type of physical embodiment of the program code. In particular, the computer-readable medium can comprise program code embodied on one or more portable storage articles of manufacture (e.g., a compact disc, a magnetic disk, a tape, etc.), on one or more data storage portions of a computing device, such as memory **18** and/or a storage system.

As used herein, it is understood that the terms "program code" and "computer program code" are synonymous and mean any expression, in any language, code or notation, of a set of instructions that cause a computing device having an information processing capability to perform a particular function either directly or after any combination of the following: (a) conversion to another language, code or notation; (b) reproduction in a different material form; and/or (c) decompression. To this extent, program code can be embodied as one or more types of program products, such as an application/software program, component software/a library of functions, an operating system, a basic I/O system/driver for a particular computing and/or I/O device, and the like. Further, it is understood that terms such as "component" and "system" are synonymous as used herein and represent any combination of hardware and/or software capable of performing some function(s).

The block diagrams in the figures illustrate the architecture, functionality, and operation of possible implementations of systems, methods and computer readable medium according to various embodiments of the present invention. In this regard, each block in the block diagrams may represent a module, segment, or portion of code, which comprises one or more executable instructions for implementing the specified logical function(s). It should also be noted that the functions noted in the blocks may occur out of the order noted in the figures. For example, two blocks shown in succession may, in fact, be executed substantially concurrently, or the blocks may sometimes be executed in the reverse order, depending upon the functionality involved. It will also be noted that each block of the block diagrams can be implemented by special purpose hardware-based systems which perform the specified functions or acts, or combinations of special purpose hardware and computer instructions.

As used herein, an element or step recited in the singular and proceeded with the word "a" or "an" should be understood as not excluding plural elements or steps, unless such exclusion is explicitly stated. Furthermore, references to "one embodiment" of the present invention are not intended to be interpreted as excluding the existence of additional embodiments that also incorporate the recited features. Moreover, unless explicitly stated to the contrary, embodiments "comprising" or "having" an element or a plurality of elements having a particular property may include additional such elements not having that property.

Although specific embodiments have been illustrated and described herein, those of ordinary skill in the art appreciate that any arrangement which is calculated to achieve the same purpose may be substituted for the specific embodiments shown and that the invention has other applications in other environments. This application is intended to cover any adaptations or variations of the present invention. The following claims are in no way intended to limit the scope of the invention to the specific embodiments described herein.

What is claimed is:

1. A method for website authentication, using at least one computer hardware device for performing the steps of:

receiving a request from a user to view a website within a graphical user interface (GUI);

generating, in response to the receiving a request, a one time password (OTP);

storing the generated OTP in a database;

displaying the generated OTP on the GUI over a first channel;

communicating a number for the user to call on a communication device over a second channel;

verifying an identity of the user by receiving an identification datum from the communication device, wherein the user sends, in response to the displaying, the identification datum using the communication device, wherein the verifying compares the identification datum with a stored identification datum in the database, wherein the identification datum is at least one of a caller ID, an account number, a password and a first geographical location;

determining a second geographical location from the request from the user to view the website and storing the second geographical location in the database;

receiving, in response to the verifying, an entered OTP from the user;

comparing the entered OTP with the generated OTP; and

communicating whether the website is authenticated.

2. The method of claim **1**, wherein the identification datum includes at least one of an identification datum automatically generated by the communication device and an identification datum input by the user.

3. The method of claim **1**, wherein the communicating includes at least one of storing a fake website in the database and alerting an authentic website administrator of the fake website.

4. A website authentication system, including a computer hardware device comprising:

a one time password (OTP) generator system for receiving a request from a user to view a website within a graphical user interface (GUI), generating, in response to the

receiving a request, a OTP, and displaying the generated OTP on the GUI over a first channel;

a system for communicating a number for the user to call on a communication device over a second channel;

a voice response unit (VRU) system for receiving at least one identification datum from a communication device, wherein the user sends, in response to the displaying, the identification datum using the communication device;

a user verification system for verifying an identity of the user by receiving an identification datum from the communication device, wherein the identification datum includes at least one of an identification datum automatically generated by the communication device and an identification datum input by the user, wherein the identification datum is at least one of a caller ID, an account number, a password and a first geographical location, and wherein the OTP generator system determines a second geographical location from the request from the user to view the website and storing the second geographical location in the database;

a comparison system for receiving, in response to the verifying, an entered OTP from the user and comparing the entered OTP with the generated OTP; and

a security alert system for communicating whether the website is authenticated.

5. The system of claim **4**, wherein the comparison system communicates whether the website is authenticated.

6. The system of claim **4**, wherein the OTP generator system stores the generated OTP in a database.

7. The system of claim **4**, wherein the verification system compares the identification datum with a stored identification datum in the database.

8. The system of claim **4**, wherein the communicating includes at least one of storing a fake website in the database and alerting an authentic website administrator of the fake website.

9. A non-transitory computer readable medium storing a program product including program code for website authentication, which when executed by a computing device, is operable to carry out a method comprising:

receiving a request from a user to view a website within a graphical user interface (GUI);

generating, in response to the receiving a request, a one time password (OTP);

storing the generated OTP in a database;

displaying the generated OTP on the GUI over a first channel;

communicating a number for the user to call on a communication device over a second channel;

verifying an identity of the user by receiving an identification datum from a communication device, wherein the user sends, in response to the displaying, the identification datum using the communication device, wherein the verifying compares the identification datum with a stored identification datum in the database, wherein the identification datum is at least one of a caller ID, an account number, a password and a first geographical location;

determining a second geographical location from the request from the user to view the website;

receiving, in response to the verifying, an entered OTP from the user;

comparing the entered OTP with the generated OTP; and

communicating whether the website is authenticated.

10. The program product of claim **9**, wherein the identification datum includes at least one of an identification datum automatically generated by the communication device and an identification datum input by the user.

* * * * *

9.2 MOBILE PHONE AND IP ADDRESS CORRELATION SERVICE


US008683609B2

(12) **United States Patent**
Bravo et al.

(10) **Patent No.: US 8,683,609 B2**
(45) **Date of Patent: Mar. 25, 2014**

(54) **MOBILE PHONE AND IP ADDRESS CORRELATION SERVICE**

(75) Inventors: **Jose F. Bravo**, Mamaroneck, NY (US); **Jeffery L. Crume**, Raleigh, NC (US)

(73) Assignee: **International Business Machines Corporation**, Armonk, NY (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 391 days.

(21) Appl. No.: **12/630,875**

(22) Filed: **Dec. 4, 2009**

(65) **Prior Publication Data**

US 2011/0138483 A1 Jun. 9, 2011

(51) **Int. Cl.**
G06F 21/00 (2013.01)

(52) **U.S. Cl.**
USPC **726/29**; 380/258

(58) **Field of Classification Search**
USPC 726/29
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,310,720	A	1/1982	Check, Jr.
5,046,082	A	9/1991	Zicker et al.
5,068,894	A	11/1991	Hoppe
5,323,465	A	6/1994	Avarne
5,457,737	A	10/1995	Wen
5,491,752	A	2/1996	Kaufman et al.
5,497,411	A	3/1996	Pellerin
5,647,388	A	7/1997	Butler, Jr. et al.
5,657,388	A	8/1997	Weiss
5,684,950	A	11/1997	Dare et al.
5,701,339	A	12/1997	Suda
5,749,052	A	5/1998	Hidem et al.
5,841,871	A	11/1998	Pinkas
5,842,124	A	11/1998	Kenagy et al.
5,892,902	A	4/1999	Clark
5,953,422	A	9/1999	Angelo et al.
5,971,272	A	10/1999	Hsiao
6,000,031	A	12/1999	Bingaman et al.
6,169,890	B1	1/2001	Vatanen
6,278,863	B1	8/2001	Mabrouki
6,308,268	B1	10/2001	Audebert

(Continued)

FOREIGN PATENT DOCUMENTS

DE	10317176	A1	11/2004
EP	1119147	A1	7/2001

(Continued)

OTHER PUBLICATIONS

Lakhia, U.S. Appl. No. 11/753,673, Office Action 1, IBMC-0208, 13 pages, Apr. 15, 2010.

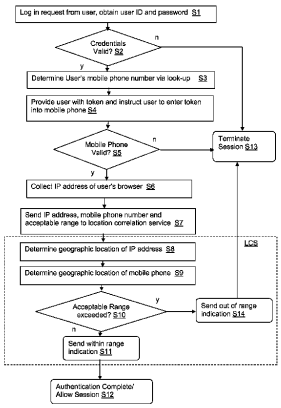
(Continued)

Primary Examiner — Gilberto Barron, Jr.
Assistant Examiner — Devin Almeida
(74) *Attorney, Agent, or Firm* — Douglas A. Lashmit; Hoffman Warnick LLC

(57) **ABSTRACT**

A system, method and program product for controlling access to a restricted item. A method is provided that includes: receiving a request for access to a restricted item at a computer system associated with a provider, said request originating from a client system; determining an IP address of the client system; determining a mobile phone number of a mobile phone associated with the requester; transmitting to a third party service provider the IP address and mobile phone number; and receiving back from the third party service provider a confirmation message indicating whether or not the IP address and mobile phone are located within an acceptable range of each other.

19 Claims, 2 Drawing Sheets



(56) **References Cited**

U.S. PATENT DOCUMENTS

6,324,271 B1 11/2001 Sawyer et al.
6,330,608 B1 12/2001 Stiles
6,334,056 B1 12/2001 Holmes et al.
6,338,140 B1 1/2002 Owens et al.
6,349,134 B1 2/2002 Katz
6,385,729 B1 5/2002 DiGiorgio et al.
6,387,729 B2 5/2002 Eng et al.
6,393,468 B1 5/2002 McGee
6,400,726 B1 6/2002 Piret et al.
6,466,780 B1 10/2002 Geiselman et al.
6,535,726 B1 3/2003 Johnson
6,584,309 B1 6/2003 Whigham
6,687,241 B1 2/2004 Goss
6,707,915 B1 3/2004 Jobst et al.
6,731,731 B1 5/2004 Ueshima
6,993,658 B1 1/2006 Engberg et al.
6,993,663 B1 1/2006 Paya et al.
7,007,301 B2 2/2006 Crosbie et al.
7,024,688 B1 4/2006 Faccin et al.
7,025,179 B2 4/2006 Shih
7,028,179 B2 4/2006 Anderson et al.
7,058,796 B2 6/2006 Lynn et al.
7,058,968 B2 6/2006 Rowland et al.
7,100,204 B1 8/2006 Myllymaki et al.
7,133,662 B2 * 11/2006 Bravo et al. 455/411
7,142,840 B1 11/2006 Geddes et al.
7,221,949 B2 5/2007 Clough
7,290,278 B2 10/2007 Cahill et al.
7,317,693 B1 1/2008 Roesch et al.
7,324,976 B2 * 1/2008 Gupta et al. 705/65
7,337,431 B1 2/2008 Barnes et al.
7,357,310 B2 4/2008 Calabrese et al.
7,360,248 B1 4/2008 Kanevsky et al.
7,376,431 B2 5/2008 Niedermeyer
7,379,921 B1 5/2008 Kiliccote
7,380,708 B1 6/2008 Kiliccote
7,447,494 B2 11/2008 Law et al.
7,480,805 B1 1/2009 Gnech et al.
7,491,308 B2 2/2009 Talieh et al.
7,519,989 B2 4/2009 Lin et al.
7,533,414 B1 5/2009 Reed et al.
7,536,634 B2 5/2009 Green et al.
7,540,022 B2 5/2009 Barari et al.
7,594,270 B2 9/2009 Church et al.
7,600,676 B1 10/2009 Rados et al.
7,609,625 B2 10/2009 Wei et al.
7,623,458 B2 11/2009 Ayyagari et al.
7,624,447 B1 11/2009 Horowitz et al.
7,665,128 B2 2/2010 Yang
7,673,334 B2 3/2010 Takemori et al.
7,715,823 B2 5/2010 Bravo et al.
7,716,742 B1 5/2010 Roesch et al.
7,757,285 B2 7/2010 Kubota
7,765,584 B2 7/2010 Roskind
7,779,465 B2 8/2010 Baker et al.
7,823,199 B1 10/2010 Rathi et al.
7,840,993 B2 11/2010 Ganesan et al.
7,845,004 B2 11/2010 Bardsley et al.
7,886,346 B2 2/2011 Sandhu et al.
7,926,108 B2 4/2011 Rand et al.
7,930,540 B2 4/2011 Ahuja et al.
7,954,150 B2 5/2011 Croft et al.
7,975,293 B2 7/2011 Yoshida et al.
8,019,995 B2 9/2011 van Bemmel
8,024,567 B2 9/2011 Han
8,050,658 B2 11/2011 Hong
8,060,915 B2 11/2011 Voice et al.
8,136,150 B2 3/2012 Hayler et al.
8,150,370 B2 4/2012 Dempo et al.
8,151,327 B2 4/2012 Eisen
8,181,248 B2 5/2012 Oh et al.
8,201,217 B1 6/2012 Begen et al.
8,254,542 B2 8/2012 Frederick
8,281,375 B2 10/2012 von Krogh
8,285,639 B2 * 10/2012 Eden et al. 705/39
8,296,823 B2 10/2012 Schubert
8,301,877 B2 10/2012 Grajek et al.
8,302,180 B1 10/2012 Gudov et al.
8,302,187 B1 10/2012 Gupta et al.
2001/0054155 A1 12/2001 Hagan et al.
2002/0069165 A1 6/2002 O'Neil
2002/0091931 A1 7/2002 Quick et al.
2002/0095588 A1 7/2002 Shigematsu et al.
2002/0178070 A1 11/2002 Leveridge
2002/0178370 A1 11/2002 Gurevich et al.
2003/0014315 A1 1/2003 Jaalinoja et al.
2003/0154382 A1 8/2003 Vicard
2003/0172272 A1 9/2003 Ehlers et al.
2004/0148520 A1 7/2004 Talpade et al.
2004/0152446 A1 8/2004 Saunders et al.
2004/0198329 A1 10/2004 Vasa
2005/0015624 A1 1/2005 Ginter et al.
2005/0018618 A1 1/2005 Mualem et al.
2005/0022020 A1 1/2005 Fremberg
2005/0060535 A1 3/2005 Bartas
2005/0075070 A1 4/2005 Crilly, Jr.
2005/0182958 A1 8/2005 Pham et al.
2005/0187934 A1 8/2005 Motsinger et al.
2005/0188423 A1 8/2005 Motsinger et al.
2005/0210251 A1 9/2005 Nyberg et al.
2006/0021031 A1 1/2006 Leahy et al.
2006/0036690 A1 2/2006 O'Neil
2006/0094403 A1 5/2006 Norefors et al.
2006/0095955 A1 5/2006 Vong et al.
2006/0288411 A1 12/2006 Garg et al.
2007/0015492 A1 1/2007 Bravo et al.
2007/0067828 A1 3/2007 Bychkov
2007/0083606 A1 4/2007 Malik et al.
2007/0084913 A1 * 4/2007 Weston 235/380
2007/0107050 A1 5/2007 Selvarajan
2007/0136573 A1 6/2007 Steinberg
2007/0136808 A1 6/2007 Xiong
2007/0143851 A1 6/2007 Nocodemus et al.
2007/0186099 A1 8/2007 Beck et al.
2007/0234426 A1 10/2007 Khanolkar et al.
2007/0261112 A1 11/2007 Todd et al.
2007/0266257 A1 11/2007 Camaisa et al.
2008/0028447 A1 1/2008 O'Malley et al.
2008/0172730 A1 7/2008 Sandhu et al.
2008/0181380 A1 7/2008 Gustave et al.
2008/0189776 A1 8/2008 Constable
2008/0209275 A1 8/2008 Kwan et al.
2008/0270301 A1 10/2008 Jones et al.
2008/0281737 A1 11/2008 Fajardo
2008/0318548 A1 12/2008 Bravo et al.
2009/0037329 A1 2/2009 Coppinger et al.
2009/0077637 A1 3/2009 Santos et al.
2009/0094682 A1 4/2009 Sage et al.
2009/0095588 A1 4/2009 Thomas
2009/0104889 A1 * 4/2009 Lotvonen et al. 455/410
2009/0106138 A1 4/2009 Smith et al.
2009/0300738 A1 12/2009 Dewe et al.
2010/0024017 A1 1/2010 Ashfield et al.
2010/0051686 A1 3/2010 Obi
2010/0095351 A1 4/2010 Liu et al.
2010/0269162 A1 10/2010 Bravo et al.
2011/0015449 A1 1/2011 Pendleton et al.
2011/0039237 A1 2/2011 Skare
2011/0138483 A1 6/2011 Bravo et al.
2011/0197070 A1 8/2011 Mizrah
2011/0225647 A1 9/2011 Dilley et al.
2011/0277024 A1 11/2011 Begley et al.
2011/0289576 A1 11/2011 Cheng
2012/0011066 A1 1/2012 Telle et al.
2012/0149334 A1 6/2012 Zhang et al.
2012/0204241 A1 8/2012 Varsavsky et al.
2012/0264405 A1 10/2012 Bravo et al.
2012/0272331 A1 10/2012 Lemaster et al.
2013/0007859 A1 1/2013 Bravo et al.

FOREIGN PATENT DOCUMENTS

GB 2456509 A 7/2009
JP 10334048 12/1998

(56) **References Cited**

FOREIGN PATENT DOCUMENTS

JP	10341224		12/1998
JP	2001111545		4/2001
WO	0109808	A1	8/2001
WO	2004079499	A2	9/2004
WO	2006103387	A1	10/2006
WO	2008147353	A1	12/2008

OTHER PUBLICATIONS

Lakhia, U.S. Appl. No. 11/753,673, Final Office Action 1, IBMC-0208, 13 pages, Oct. 8, 2010.
Lakhia, U.S. Appl. No. 11/753,673, Office Action 2, IBMC-0208, 15 pages, Dec. 22, 2011.
Lakhia, U.S. Appl. No. 11/753,673, Notice of Allowance 1, IBMC-0208, 11 pages, Jun. 18, 2012.
Lakhia, U.S. Appl. No. 11/753,673, Notice of Allowance 2, IBMC-0208, 14 pages, Jan. 8, 2013.
Megeed, U.S. Appl. No. 12/423,928, Office Action 1, IBMC-0326, 21 pages, Aug. 25, 2011.
Megeed, U.S. Appl. No. 12/423,928, Final Office Action 1, IBMC-0326, 20 pages, Nov. 10, 2011.
Megeed, U.S. Appl. No. 12/423,928, Office Action 2, IBMC-0326, 20 pages, Jun. 8, 2012.
Megeed, U.S. Appl. No. 12/423,928, Notice of Allowance 1, IBMC-0326, 10 pages, Sep. 25, 2012.
Megeed, U.S. Appl. No. 12/423,928, Notice of Allowance 2, IBMC-0326, 19 pages, Dec. 4, 2012.
Bibbee, U.S. Appl. No. 11/765,193, Office Action 1, 15 pages, Feb. 18, 2010.
Bibbee, U.S. Appl. No. 11/765,193, Office Action 2, 14 pages, Nov. 29, 2010.
Bibbee, U.S. Appl. No. 11/765,193, Office Action 3, 18 pages, Sep. 19, 2011.
Bibbee, U.S. Appl. No. 11/765,193, Final Office Action 1, 15 pages, Jul. 30, 2010.
Bibbee, U.S. Appl. No. 11/765,193, Final Office Action 2, 17 pages, May 12, 2011.
Bibbee, U.S. Appl. No. 11/765,193, Final Office Action 3, 18 pages, Apr. 16, 2012.
Tran, U.S. Appl. No. 11/524,340, Office Action, 9 pages, Jul. 29, 2009.
Tran, U.S. Appl. No. 11/524,340, Office Action, 19 pages, Oct. 31, 2008.
Tran, U.S. Appl. No. 11/524,340, Notice of Allowance, 11 pages, Dec. 29, 2009.
Tran, U.S. Appl. No. 11/524,340, Office Action, 7 pages, Apr. 29, 2009.
Tran, U.S. Appl. No. 11/524,340, Office Action, 22 pages, May 27, 2008.
Juels, "Strengthening EPC Tags Against Cloning", WISE '05, Sep. 2, 2005, pp. 67-75.
Kumaraguru et al., "Getting Users to Pay Attention to Anti-Phishing Education: Evaluation of Retention and Transfer", APWG eCrime Researchers Summit, Oct. 4-5, 2007, Pittsburgh, PA pp. 70-81.
Adida, "BeamAuth: Two-Factor Web Authentication with a Bookmark", CCS '07, Oct. 29-Nov. 2, 2007, Alexandria, VA, ACM 978-1-59593-703-2/07/0010, pp. 48-57.
Nassar et al., "Holistic VoIP Intrusion Detection and Prevention System", IPTCOMM '07, ACM 2007, pp. 1-9.
Stoll et al., "Sesame: Informing User Security Decisions with System Visualization", CHI 2008 Proceedings, Am I Safe, Apr. 5-10, 2008, Florence, Italy, pp. 1045-1054.
Lee et al., "A Resilient Packet-Forwarding Scheme against Maliciously Packet-Dropping Nodes in Sensor Networks" SASN '06, Oct. 30, 2005, ACM 1-59593-544-J/06/0010, pp. 59-69.
Deng et al., "Defending Against Redirect Attacks in Mobile IP", CCS '02, Nov. 18-22, 2002, ACM 1-58113-612-9/02/0011, pp. 59-67.
Kaafar et al., "Real attacks on virtual networks: Vivaldi out of tune", SIGCOMM '06 Workshops, Sep. 11-15, 2006, ACM 1-59593-417-0/06/0009, pp. 139-146.
Geneiatakis et al., "Survey of Security Vulnerabilities in Session Initiation Protocol", 3rd Quarter 2006, vol. 8, No. 3, IEEE Communications Surveys & Tutorials, pp. 68-81.
"Prevent Online Banking Fraud", Dec. 7, 2010, http://www.phonefactor.com/products/transaction-verification, 1 pages.
Bonzo, U.S. Appl. No. 11/776,619, Office Action, Sep. 30, 2009, 12 pages.
Bonzo, U.S. Appl. No. 11/776,619, Notice of Allowance, Apr. 29, 2010, 10 pages.
Alicherry et al., "DoubleCheck: Multi-ath Verification Against Man-in-the-Middle Attack", IEEE 2009, pp. 557-563.
Koo et al., "VoIP Interception in P2P SIP Environment", 2010 IEEEE, vol. 1, pp. 331-334.
Kopsidas et al., "Voice Interactive Personalized Security (VoIPSEC) protocol: Fortify Internet telephony by providing end-to-end security through inbound key exchange and biometric verification", 2006 IEEE, 10 pgs.
Leung, "Depress Phishing by CAPTCHA with OTP", Department of Information Engineering the Chinese University of Hong Kong, IEEE 2009, 6 pgs.
Viral, U.S. Appl. No. 11/753,673, Notice of Allowance, Aug. 21, 2012, 7 pages.
Lakhia, U.S. Appl. No. 13/432,956, Office Action 1, IBMC-0208-CON, Feb. 14, 2013, 26 pages.
Gee, U.S. Appl. No. 13/084,823, Office Action, IBMC-0395, Mar. 11, 2013, 8 pages.
Ma et al., "Beyond Blacklists: Learning to Detect Malicious Web Sites from Suspicious URLs", KDD '09, Jul. 28-Jul. 1, 2009, pp. 1245-1253.
Lakhia, U.S. Appl. No. 13/432,956, Notice of Allowance & Fees Due, Apr. 15, 2013, 27 pages.
Bibbee, U.S. Appl. No. 11/765,193, Examiner's Answer, Apr. 16, 2013, 20 pages.
Vaughan, U.S. Appl. No. 12/423,928, Notice of Allowance & Fees Due, Jul. 11, 2013, 25 pages.
Lakhia, U.S. Appl. No. 11/753,673, Notice of Allowance & Fees Due, dated May 10, 2013, 28 pages.

* cited by examiner

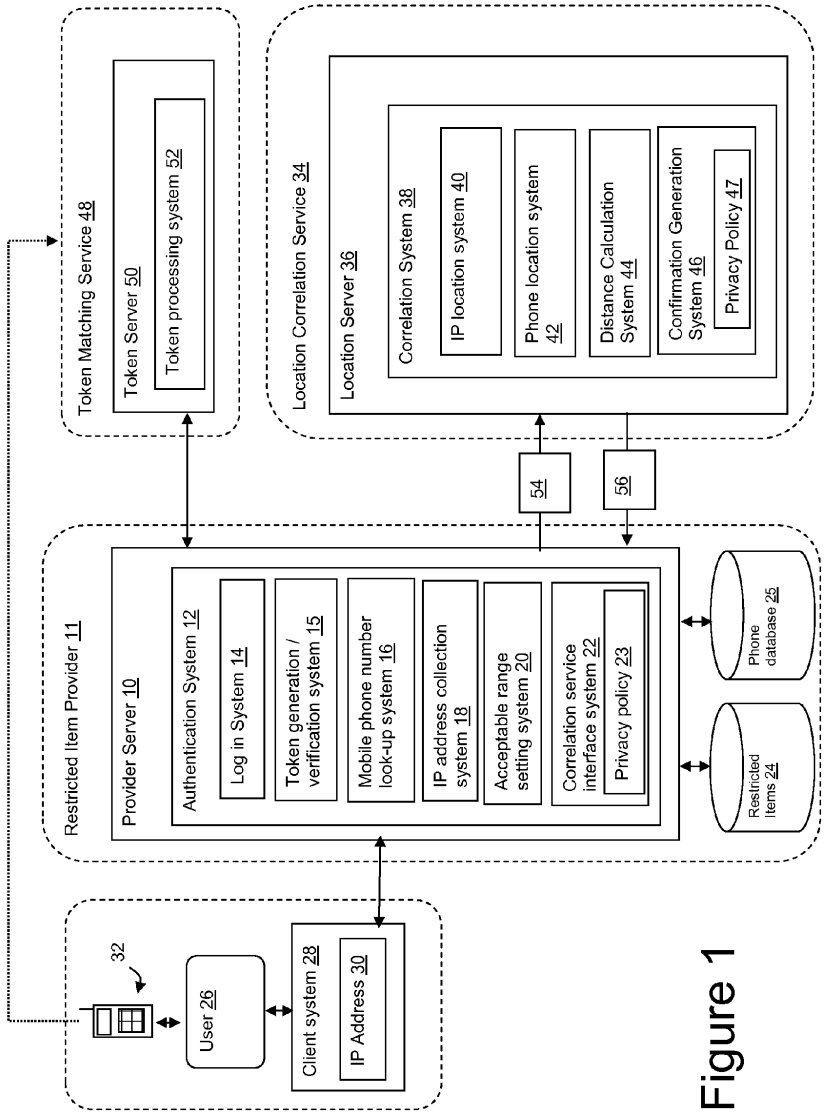

Token Matching Service 48
Token Server 50
Token processing system 52
Location Correlation Service 34
Location Server 36
Correlation System 38
IP location system 40
Phone location system 42
Distance Calculation System 44
Confirmation Generation System 46
Privacy Policy 47
54
56
Restricted Item Provider 11
Provider Server 10
Authentication System 12
Log in System 14
Token generation / verification system 15
Mobile phone number look-up system 16
IP address collection system 18
Acceptable range setting system 20
Correlation service interface system 22
Privacy policy 23
Phone database 25
Restricted Items 24
32
User 26
Client system 28
IP Address 30

Figure 1

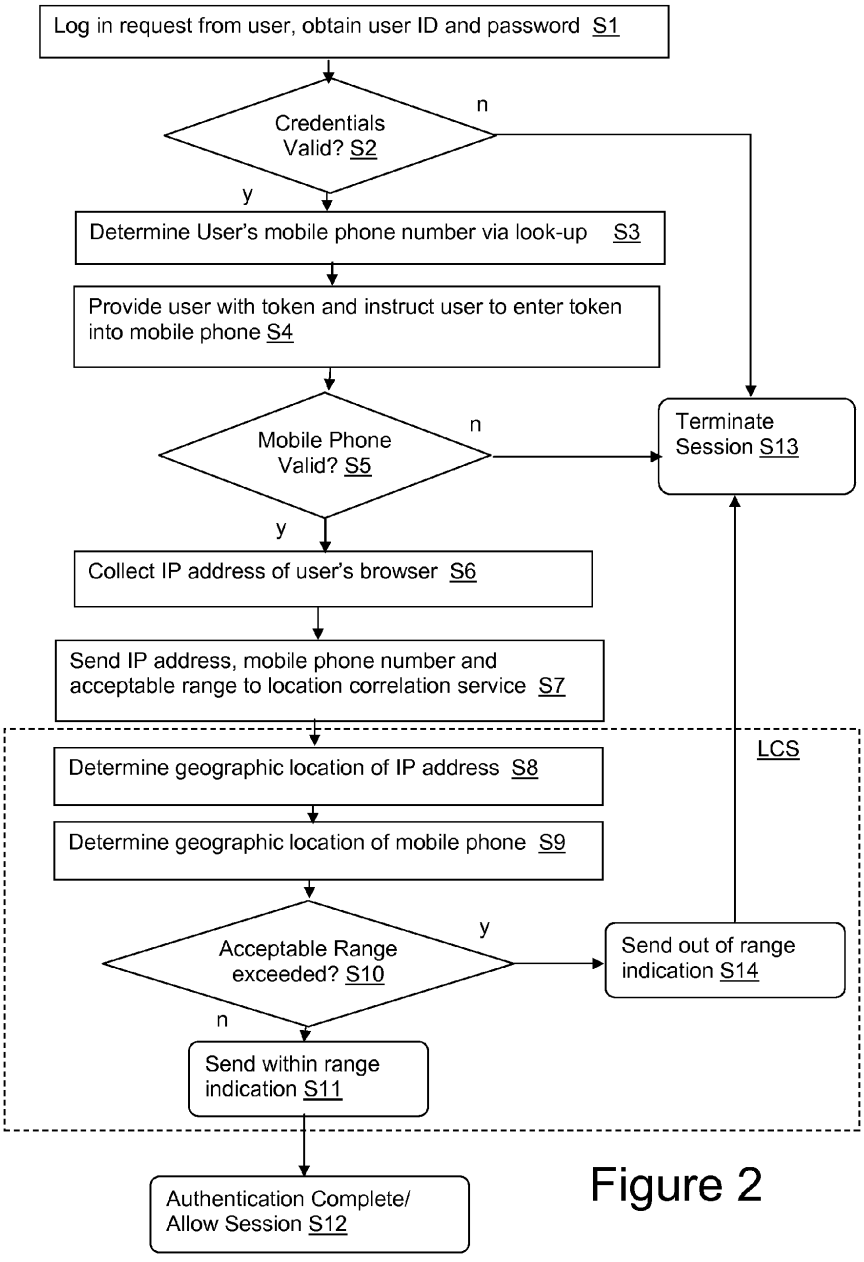

Log in request from user, obtain user ID and password S1
Credentials Valid? S2
n
y
Determine User's mobile phone number via look-up S3
Provide user with token and instruct user to enter token into mobile phone S4
Mobile Phone Valid? S5
n
Terminate Session S13
y
Collect IP address of user's browser S6
Send IP address, mobile phone number and acceptable range to location correlation service S7
LCS
Determine geographic location of IP address S8
Determine geographic location of mobile phone S9
Acceptable Range exceeded? S10
y
Send out of range indication S14
n
Send within range indication S11
Authentication Complete/ Allow Session S12

Figure 2

MOBILE PHONE AND IP ADDRESS CORRELATION SERVICE

FIELD OF THE INVENTION

This disclosure is related generally to detecting man-in-the-middle attacks, and more particularly to an authentication infrastructure having a third party location correlation service that ensures privacy protections.

BACKGROUND OF THE INVENTION

In certain instances it is useful to know if a physical location of a mobile device associated with a user correlates to the location of a second device being used by the user. By comparing the geographical locations of the two devices, the user can be authenticated. If the two locations are not physically near each other, it may be assumed that a man-in-the-middle attack is underway as the transaction appears to emanate from a location that is distant from the actual user.

One of the issues of utilizing location correlation is that it allows for tracking and collection of precise location details of individuals which, from a privacy perspective, may be undesirable.

SUMMARY OF THE INVENTION

The present invention provides an authentication infrastructure in which a third party location correlation service provider is implemented separately from a restricted item provider (i.e., provider) to ensure privacy for users.

In one embodiment, there is a method for controlling access to a restricted item, comprising: receiving a request from a requester for access to a restricted item at a computer system associated with a provider, said request originating from a client system; determining an IP address of the client system; determining a mobile phone number of a mobile phone associated with the requester; transmitting to a third party service provider the IP address and mobile phone number; and receiving back from the third party service provider a confirmation message indicating whether or not the IP address and mobile phone are located within an acceptable range of each other.

In a second embodiment, there is a system for controlling access to a restricted item, comprising: a login system for receiving a request from a requester to a restricted item, said request originating from a client system; a system for determining an IP address of the client system; a system for determining a mobile phone number of a mobile phone associated with the requester; a system for transmitting to a third party service provider the IP address and mobile phone number; and a system for inputting from the third party service provider a confirmation message indicating whether or not the IP address and mobile phone are located within an acceptable range of each other.

In a third embodiment, there is a computer readable storage medium having a program product for controlling access to a restricted item, comprising: program code for receiving a request from a requester to a restricted item, said request originating from a client system; program code for determining an IP address of the client system; program code for determining a mobile phone number of a mobile phone associated with the requester; program code for transmitting to a third party service provider the IP address and mobile phone number; and program code for inputting from the third party service provider a confirmation message indicating whether or not the IP address and mobile phone are located within an acceptable range of each other.

In a fourth embodiment, there is a method for deploying a system for controlling access to a restricted item, comprising: providing a computer infrastructure being operable to: receive a request from a requester for access to a restricted item at a computer system associated with a provider, said request originating from a client system; determine an IP address of the client system; determine a mobile phone number of a mobile phone associated with the requester; transmit to a third party service provider the IP address and mobile phone number; and receive back from the third party service provider a confirmation message indicating whether or not the IP address and mobile phone are located within an acceptable range of each other.

A location correlation service as described herein could be offered by mobile phone providers to merchants, banks and other organizations for any authentication purposes, e.g., processing credit cards for e-commerce, e-banking transactions, content access, etc. Companies could use the service to authenticate business partners accessing their organization's infrastructure via a VPN or extranet web site. The illustrative aspects of the present invention are designed to solve the problems herein described and other problems not discussed.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other features of this invention will be more readily understood from the following detailed description of the various aspects of the invention taken in conjunction with the accompanying drawings.

FIG. **1** depicts an illustrative authentication infrastructure in accordance with an embodiment of the present invention.

FIG. **2** depicts a flow chart showing a method in accordance with an embodiment of the present invention.

The drawings are merely schematic representations, not intended to portray specific parameters of the invention. The drawings are intended to depict only typical embodiments of the invention, and therefore should not be considered as limiting the scope of the invention. In the drawings, like numbering represents like elements.

DETAILED DESCRIPTION OF THE INVENTION

The described embodiments provide solutions for maintaining privacy when location information is required to authenticate a user attempting to access a restricted item over a network from a restricted item provider, i.e., "provider." The provider may be any entity that controls access to restricted items, e.g., a bank, a business, a web site, a server, etc. In some authentication embodiments, such as that described in US 2008/0318548 US1, published on Dec. 25, 2008, entitled "Method and System for Strong Authentication and Defense against Man-In-the-Middle Attacks," the contents of which are hereby incorporated by reference, the location of the user's mobile phone and the location of the user's computer IP address are examined by the restricted item provider to determine if the two are proximately located.

The present approach provides a third party location correlation service that can be tuned to limit the exposure of precise location details of the user while still providing the necessary information to authenticate the user to the restricted item provider. Namely, the third party location correlation service may be utilized to provide only a yes/no confirmation as to whether a mobile phone is within a specified range of a given IP address. Thus, the restricted item

provider can thwart man-in-the-middle attacks without ever having to know any location information of the user.

Referring now to FIG. **1**, an illustrative embodiment of an authentication infrastructure is shown that generally includes a restrictive item provider **11**, a token matching service **48** and a location correlation service **34**. Restricted item provider **11** generally comprises any entity that provides access to restricted item **24** via a network such as the World Wide Web (Web) to a user **26** via a client system **28**. Client system **28** may comprise any device, software or system, such as a computer and browser, handheld device, ATM machine, transaction processor, etc., that utilizes a unique network identifier, such as an IP (Internet Protocol) address or the like to interface with the restricted item provider **11** via a provider server **10**.

Within this infrastructure, authentication of user **26** by restricted item provider **11** is implemented as follows. Provider server **10** includes an authentication system **12**, which may for example be implemented as any combination of hardware and software (i.e., a computer system and/or a program product). Authentication system **12** generally includes: a log in system **14**; a token generation/verification system **15**; a mobile phone number look-up system **16**; an IP address collection system **18**; an acceptable range setting system **20**; and a correlation service interface system **22**. When user **26** seeks to access a restricted item **24** from restricted item provider **11**, user **26** points their client system **28** to the provider server **12** (e.g., by entering a Web address into a browser). Restricted item **24** may comprise any item, e.g., data, object, program, communication channel, etc., for which authorization is required. Common examples of restricted items **24** include account data, transaction systems, subscription-based content, etc.

When attempting to access the provider server **10**, user **26** is first presented with a log in system **14**, where the user is verified, e.g., by entering a user ID and password. Once the user's ID and password are verified, token generation/verification system **15** generates a one-time token that is forwarded back to the user **26** via the client system **28**. The user **26** is then prompted to enter the one time token into the user's mobile phone **32**, which is forwarded to token matching service **48** via a cellular network or the like. In a parallel process, a mobile phone number look-up system **16** retrieves a previously stored (i.e., pre-registered) mobile phone number of the user **26** from a phone database **25**. The mobile phone number of the user **26** and the generated one time token are also forwarded to the token matching service **48** from the provider server **10**.

A token server **50** provides a token processing system **52** that compares the phone number (e.g., using caller ID) and token obtained from the user **26** via the mobile phone **32** with the phone number and token information separately obtained from the authentication system **12**. If the data matches, this then verifies that the mobile phone **32** being used to submit the token belongs to the user **26**. If the data does not match, this then indicates that a man-in-the-middle attack or other type of unauthorized access may be occurring since an unauthorized mobile phone was utilized to submit the token. Note that some or all of the processing being done by token matching service **48** could be done by a third party provider or by the restricted item provider **11** itself, e.g., at the provider server **10**. In addition, it is understood that any type of token may be utilized, e.g., an alphanumeric code that user **26** types into their phone, a password that the user speaks, etc. A detailed description of token processing is disclosed in U.S. Pat. No. 7,133,662 issued on Nov. 7, 2006 to Bravo et al., entitled "Method and apparatus for restricting access of a user using a cellular telephone," the contents of which is hereby incorporated by reference.

Assuming the token is verified, a further authentication process is utilized to ensure that the mobile phone **32** is located proximate to the client system **28**. To implement this, IP address collection system **18** collects the IP address **30** of the client system **28**, e.g., during the log in procedure. An acceptable distance between the mobile phone **32** and the client system **28** may be set by acceptable range setting system **20**. Given that current technology does not always allow for pinpointing an exact location of a mobile phone **32** or IP address **30** of client system **28**, authentication system **12** provides this mechanism for setting an acceptable range value (e.g., 10 miles). By allowing the restricted item provider **11** to set this value, provider **11** can dictate their own level of risk tolerance.

Once the user's mobile phone number and IP address **30** are determined, they are packaged and sent to location correlation server **34** with the acceptable range value in a transmission **54** by correlation service interface system **22**. As noted herein, an aspect of this disclosure involves ensuring privacy for the user **26**. More particularly, the user's location based on their mobile phone **32** should not be tracked and/or stored by the restricted item provider **11** or other third parties. Correlation service interface system **22** ensures this feature by utilizing a privacy policy **23** requiring a third party service to simply confirm whether or not the acceptable distance between the mobile phone **32** and the client system **28** is met. The privacy policy **23** does not allow for the collection of actual mobile phone location data by the restricted item provider **11** from the location correlation service **34**.

Accordingly, location correlation service **34** must be implemented as a separate disparate entity relative to restricted item provider **11**. In one embodiment, location correlation service **34** may be implemented by a cellular provider as a service for organizations, such as banks and other businesses. Location correlation service **34** generally includes a location server **36** that has a correlation system **38** for confirming whether a mobile phone is located proximate an IP address. Correlation system **38** includes an IP location system **40** for determining a geographic location of an IP address. Such systems are readily known (e.g., www.geobytes.com/IPlocator.htm). Phone location system **42** utilizes any known means for locating a mobile phone based on the phone number. Examples include cell tower triangulation, GPS, etc. Once correlation system **38** ascertains the geographic location of both the IP address **30** and mobile phone **32**, distance calculation system **44** determines a distance between the two, e.g., based on longitude and latitude. Confirmation generation system **46** then determines if the calculated distance is less than the acceptable range value provided by the restricted item provider **11**. A confirmation message **56** (e.g., yes or no) is then returned to correlation service interface system **22** of the restricted item provider **11**. If the proximity of the mobile phone **32** and the IP address **30** is confirmed as with the acceptable range, authentication system **12** can then allow access to the restricted item **24** for the user **26**. Otherwise, the user **26** is denied access.

Confirmation generation system **46** may likewise include a privacy policy **47** that ensures that only a simple confirmation message **56** will be returned to the requesting party. Privacy policy **47** may also enforce other privacy measures, such that the information handled by the correlation system **38** will be disposed of in an acceptable manner. The privacy policies **23**

and **47** may be exchanged using, e.g., P3P protocol, prior to, or as part of, the transaction to ensure that the required level of privacy will be met.

FIG. **2** depicts a flow chart showing an illustrative method of a user being authenticated by a provider. At S**1**, a log in request is obtained from a user at a provider's server, e.g., by pointing a browser at the log in page, where a user ID and password are collected from the user. At S**2**, a check is made to determine if the credentials (i.e., user ID and password) are valid. If no, the session is terminated at S**13**. If yes, then the mobile number of the user is determined by the provider via a look-up, e.g., from a provider's database, at S**3**. At S**4**, the user is provided a one time token from the provider, which the user then enters into his or her mobile phone, e.g., using the keypad. At S**5**, a service (e.g., a cellular provider) receives the token and the user's phone number via caller ID, and compares it with the phone number and token provided to the user by the provider. If they do not match, a man-in-the middle attack is suspected since an invalid phone is being used to enter the token and the session is terminated at S**13**. If they do match, the mobile phone is deemed valid (i.e., it belongs to or is authorized for the user) and the IP address of the user's browser is collected at S**6**. Note that the IP address of the browser can be collected earlier, e.g., during log in.

Next, at S**7**, the IP address, the mobile phone number and the acceptable range is sent to a location correlation service (LCS). The acceptable range is determined in this case by the provider based on a risk tolerance of the provider. However, it could be set by the LCS. As noted, because of the need for privacy, the LCS is a separate entity from the provider. The LCS determines the geographic location of the IP address and mobile phone at S**8** and S**9**. A physical distance between the two is calculated by the LCS using any technique and a determination is then made whether the two are located within the acceptable range at S**10**. The acceptable range, as well as the determined distance between the two, may be provided/calculated in miles, kilometers, longitudinal/latitudinal coordinates, etc.

If the two are not within the acceptable range, an "out of range" indication is sent back to the provider at S**14** and the session is terminated at S**13**. If the acceptable range is not exceeded, then a "within range" indication is sent to the provider at S**11** and the user is fully authenticated and the session is allowed at S**12**.

Note that while the embodiments are described with reference to a mobile phone, the invention may be implemented with any device that has a unique discoverable identifier (e.g., phone number, email address, IP address, etc.) and can transmit a token to a token service provider.

Referring again to FIG. **1**, it is understood that each of the authentication system **12**, token server **50** and location server **36** may be implemented using any type of computing device (i.e., computer system). Such a computing device generally includes a processor, input/output (I/O), memory, and bus. The processor may comprise a single processing unit, or be distributed across one or more processing units in one or more locations, e.g., on a client and server. Memory may comprise any known type of data storage, including magnetic media, optical media, random access memory (RAM), read-only memory (ROM), a data cache, a data object, etc. Moreover, memory may reside at a single physical location, comprising one or more types of data storage, or be distributed across a plurality of physical systems in various forms.

I/O may comprise any system for exchanging information to/from an external resource. External devices/resources may comprise any known type of external device, including a monitor/display, speakers, storage, another computer system, a hand-held device, keyboard, mouse, voice recognition system, speech output system, printer, facsimile, pager, etc. The bus provides a communication link between each of the components in the computing device and likewise may comprise any known type of transmission link, including electrical, optical, wireless, etc. Although not shown, additional components, such as cache memory, communication systems, system software, etc., may be incorporated.

Access may be provided over a network such as the Internet, a local area network (LAN), a wide area network (WAN), a virtual private network (VPN), etc. Communication could occur via a direct hardwired connection (e.g., serial port), or via an addressable connection that may utilize any combination of wireline and/or wireless transmission methods. Moreover, conventional network connectivity, such as Token Ring, Ethernet, WiFi or other conventional communications standards could be used. Still yet, connectivity could be provided by conventional TCP/IP sockets-based protocol. In this instance, an Internet service provider could be used to establish interconnectivity. Further, as indicated above, communication could occur in a client-server or server-server environment.

It should be appreciated that the teachings of the present invention could be offered as a business method on a subscription or fee basis. For example, a computer system comprising a correlation system **38** and/or token processing system **52** could be created, maintained and/or deployed by a service provider that offers the functions described herein for customers. That is, a service provider could offer to deploy or provide the ability to provide authentication as described above.

It is understood that in addition to being implemented as a system and method, the features may be provided as one or more program products stored on computer-readable storage mediums, which when run, enables one or more computer systems to provide authentication as described. To this extent, the computer-readable storage medium may include program code, which implements the processes and systems described herein. It is understood that the term "computer-readable medium" comprises one or more of any type of physical embodiment of the program code. In particular, the computer-readable medium can comprise program code embodied on one or more portable storage articles of manufacture (e.g., a compact disc, a magnetic disk, a tape, etc.), on one or more data storage portions of a computing device, such as memory and/or a storage system.

As used herein, it is understood that the terms "program code" and "computer program code" are synonymous and mean any expression, in any language, code or notation, of a set of instructions that cause a computing device having an information processing capability to perform a particular function either directly or after any combination of the following: (a) conversion to another language, code or notation; (b) reproduction in a different material form; and/or (c) decompression. To this extent, program code can be embodied as one or more types of program products, such as an application/software program, component software/a library of functions, an operating system, a basic I/O system/driver for a particular computing and/or I/O device, and the like. Further, it is understood that terms such as "component" and "system" are synonymous as used herein and represent any combination of hardware and/or software capable of performing some function(s).

The block diagrams in the figures illustrate the architecture, functionality, and operation of possible implementations of systems, methods and computer program products according to various embodiments of the present invention. In this

regard, each block in the block diagrams may represent a module, segment, or portion of code, which comprises one or more executable instructions for implementing the specified logical function(s). It should also be noted that the functions noted in the blocks may occur out of the order noted in the figures. For example, two blocks shown in succession may, in fact, be run substantially concurrently, or the blocks may sometimes be run in the reverse order, depending upon the functionality involved. It will also be noted that each block of the block diagrams can be implemented by special purpose hardware-based systems which perform the specified functions or acts, or combinations of special purpose hardware and computer instructions.

Although specific embodiments have been illustrated and described herein, those of ordinary skill in the art appreciate that any arrangement which is calculated to achieve the same purpose may be substituted for the specific embodiments shown and that the invention has other applications in other environments. This application is intended to cover any adaptations or variations of the present invention. The following claims are in no way intended to limit the scope of the invention to the specific embodiments described herein.

What is claimed is:

1. A method for controlling access to a restricted item, the method comprising:

receiving a request from a requester for access to a restricted item at a computer system associated with a provider, said request originating at a client system;

determining an IP address of the client system using the computer system associated with the provider;

receiving a telephonic communication from a mobile phone associated with the requester using the computer system associated with the provider,

wherein the requester initiates the telephonic communication using the mobile phone;

determining a geographical location of the mobile phone based on the requester-initiated telephonic communication using the mobile phone;

determining a mobile phone number of the mobile phone associated with the requester using the computer system associated with the provider;

transmitting to a third party service provider, distinct from the computer system associated with the provider, the IP address, the mobile phone number, the geographical location of the mobile phone and an acceptable range,

wherein the acceptable range includes a predetermined distance between the mobile phone and the client system; and

receiving back from the third party service provider a confirmation message indicating whether the IP address and the mobile phone are located within the acceptable range of each other, wherein the third party service provider determines whether the IP address and the mobile phone are located within the acceptable range of each other based on the transmitted IP address, the geographical location of the mobile phone and the mobile phone number.

2. The method of claim **1**, further comprising:

providing a token via the client system to the requester;

prompting the requester to transmit said token via the mobile phone associated with the requester;

verifying that the token was transmitted by the mobile phone associated with the requester.

3. The method of claim **1**, further comprising verifying a user ID and password of the requester.

4. The method of claim **1**, further comprising:

ensuring that a privacy policy is in place to guarantee that no location data of the mobile phone associated with the requester will be provided to the provider.

5. The method of claim **1**, wherein the mobile phone number of the mobile phone associated with the requester is pre-registered with the provider.

6. The method of claim **1**, further comprising authenticating the requester to allow access to the restricted item in response to a confirmation message that verifies that the mobile phone and IP address are located within the acceptable range of each other.

7. A computer system comprising:

at least one computing device configured to control access to a restricted item, by performing actions including:

receiving a request from a requester to a restricted item, said request originating from a client system;

determining an IP address of the client system;

receiving a telephonic communication from a mobile phone associated with the requester using the computer system associated with the provider,

wherein the requester initiates the telephonic communication using the mobile phone;

determining a geographical location of the mobile phone based on the requester-initiated telephonic communication using the mobile phone;

determining a mobile phone number of the mobile phone associated with the requester;

transmitting to a third party service provider, distinct from the at least one computing device, the IP address, the mobile phone number, the geographical location of the mobile phone and an acceptable range,

wherein the acceptable range includes a predetermined distance between the mobile phone and the client system; and

receiving, from the third party service provider, a confirmation message indicating whether the IP address and the mobile phone are located within the acceptable range of each other, wherein the third party service provider determines whether the IP address and the mobile phone are located within the acceptable range of each other based on the transmitted IP address, the geographical location of the mobile phone and the mobile phone number.

8. The computer system of claim **7**, further comprising:

providing a token to the requester via the client system;

prompting the requester to transmit said token via the mobile phone associated with the requester; and

verifying that the token was transmitted by the mobile phone associated with the requester.

9. The computer system of claim **7**, further comprising verifying a user ID and password of the requester.

10. The computer system of claim **7**, further comprising:

a privacy policy that guarantees that no location data of the mobile phone associated with the requester will be provided to the provider.

11. The computer system of claim **7**, wherein the mobile phone number of the mobile phone associated with the requester is pre-registered with the provider.

12. The computer system of claim **7**, further comprising authenticating the requester to allow access to the restricted item in response to a confirmation message that verifies that the mobile phone and IP address are located within the acceptable range of each other.

13. A non-transitory computer readable medium having a program product for controlling access to a restricted item,

which when executed by at least one computing device, causes the at least one computing device to perform actions including:

receiving a request from a requester to a restricted item, said request originating from a client system;

determining an IP address of the client system;

receiving a telephonic communication from a mobile phone associated with the requester using the computer system associated with the provider,

wherein the requester initiates the telephonic communication using the mobile phone;

determining a geographical location of the mobile phone based on the requester-initiated telephonic communication using the mobile phone;

determining a mobile phone number of the mobile phone associated with the requester;

transmitting to a third party service provider the IP address, the mobile phone number, the geographical location of the mobile phone and an acceptable range,

wherein the acceptable range includes a predetermined distance between the mobile phone and the client system; and

receiving from the third party service provider a confirmation message indicating whether the IP address and the mobile phone are located within the acceptable range of each other, wherein the third party service provider determines whether the IP address and the mobile phone are located within the acceptable range of each other based on the transmitted IP address, the geographical location of the mobile phone and the mobile phone number.

14. The non-transitory computer readable medium of claim **13**, further causing the at least one computing device to perform actions including:

providing a token to the requester via the client system;

prompting the requester to transmit said token via the mobile phone associated with the requester; and

verifying that the token was transmitted by the mobile phone associated with the requester.

15. The non-transitory computer readable medium of claim **13**, further causing the at least one computing device to perform actions including:

verifying a user ID and password of the requester.

16. The non-transitory computer readable medium of claim **13**, further causing the at least one computing device to perform actions including:

a privacy policy that guarantees that no location data of the mobile phone associated with the requester will be provided to the provider.

17. The non-transitory computer readable medium of claim **13**, wherein the mobile phone number of the mobile phone associated with the requester is pre-registered with the provider.

18. The non-transitory computer readable medium of claim **13**, further causing the at least one computing device to perform actions including:

authenticating the requester to allow access to the restricted item in response to a confirmation message that verifies that the mobile phone and IP address are located within the acceptable range of each other.

19. A method for deploying a system for controlling access to a restricted item, comprising:

providing a computer infrastructure being operable to:

receive a request from a requester for access to a restricted item at a computer system associated with a provider, said request originating from a client system;

determine an IP address of the client system;

receive a telephonic communication from a mobile phone associated with the requester using the computer system associated with the provider,

wherein the requester initiates the telephonic communication using the mobile phone;

determine a geographical location of the mobile phone based on the requester- initiated telephonic communication using the mobile phone;

determine a mobile phone number of the mobile phone associated with the requester;

transmit to a third party service provider, distinct from the computer infrastructure, the IP address, the mobile phone number, the geographical location of the mobile phone, and an acceptable range,

wherein the acceptable range includes a predetermined distance between the mobile phone and the client system; and

receive back from the third party service provider a confirmation message indicating whether the IP address and the mobile phone are located within the acceptable range of each other, wherein the third party service provider determines whether the IP address and the mobile phone are located within the acceptable range of each other based on the transmitted IP address, the geographical location of the mobile phone and the mobile phone number.

* * * * *

9.3 Detecting Man-in-the-Middle Attacks in Electronic Transactions Using Prompts


US008917826B2

(12) **United States Patent**
Bravo et al.

(10) **Patent No.: US 8,917,826 B2**
(45) **Date of Patent: Dec. 23, 2014**

(54) **DETECTING MAN-IN-THE-MIDDLE ATTACKS IN ELECTRONIC TRANSACTIONS USING PROMPTS**

(75) Inventors: **Jose F. Bravo**, Mamaroneck, NY (US); **Jeffery L. Crume**, Raleigh, NC (US)

(73) Assignee: **International Business Machines Corporation**, Armonk, NY (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 217 days.

(21) Appl. No.: **13/562,491**

(22) Filed: **Jul. 31, 2012**

(65) **Prior Publication Data**

US 2014/0037074 A1 Feb. 6, 2014

(51) **Int. Cl.**
H04M 1/64 (2006.01)
G06Q 20/00 (2012.01)

(52) **U.S. Cl.**
USPC **379/88.01**; 705/75

(58) **Field of Classification Search**
CPC G06Q 10/10; G06Q 20/00; G06Q 20/10; G06Q 20/382; G06Q 20/401; G06Q 20/4016; G06Q 20/403; G06Q 40/02; G06Q 40/04; G07F 17/32; G07F 17/3218; G07F 17/3223; G07F 17/3286; H04H 20/78
USPC 379/67.01; 705/64, 75, 14.51
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,310,720 A 1/1982 Check, Jr.
5,046,082 A 9/1991 Zicker et al.
5,068,894 A 11/1991 Hoppe
5,323,465 A 6/1994 Avarne
5,457,737 A 10/1995 Wen
5,491,752 A 2/1996 Kaufman et al.
5,497,411 A 3/1996 Pellerin
5,657,388 A 8/1997 Weiss

(Continued)

FOREIGN PATENT DOCUMENTS

DE 10317176 A1 11/2004
EP 1119147 A1 7/2001

(Continued)

OTHER PUBLICATIONS

Bibbee, U.S. Appl. No. 11/765,193, Examiner's Answer, Apr. 16, 2013, 20 pages.

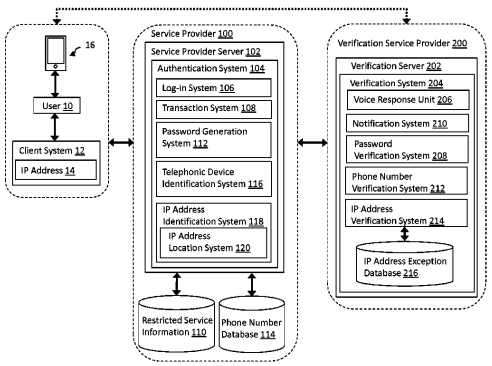
(Continued)

Primary Examiner — Fan Tsang
Assistant Examiner — Solomon Bezuayehu
(74) *Attorney, Agent, or Firm* — Douglas A. Lashmit; Hoffman Warnick LLC

(57) **ABSTRACT**

Aspects of the invention provide a solution for detecting man-in-the-middle attacks in electronic transactions using prompts. One embodiment includes a method for authenticating an electronic transaction. The method includes: receiving an electronic transaction request from a user, determining an IP address associated with a client system from which the electronic transaction request originates, providing the user with a password associated with the electronic transaction request, receiving a telephonic communication from a telephonic device associated with the user, prompting the user, via a voice response unit, to input the password using the telephonic device, authenticating the user by comparing the inputted password and the provided password, determining a probable location of the user based on the determined IP address of the client system, communicating to the user the probable location of the user based on the determined IP address, and prompting the user to confirm the probable location of the user.

21 Claims, 3 Drawing Sheets



(56) **References Cited**

U.S. PATENT DOCUMENTS

5,684,950 A 11/1997 Dare et al.
5,701,339 A 12/1997 Suda
5,749,052 A 5/1998 Hidem et al.
5,841,871 A 11/1998 Pinkas
5,842,124 A 11/1998 Kenagy et al.
5,892,902 A 4/1999 Clark
5,953,422 A 9/1999 Angelo et al.
5,971,272 A 10/1999 Hsiao
6,000,031 A 12/1999 Bingaman et al.
6,169,890 B1 1/2001 Vatanen
6,278,863 B1 8/2001 Mabrouki
6,308,268 B1 10/2001 Audebert
6,324,271 B1 11/2001 Sawyer et al.
6,330,608 B1 12/2001 Stiles
6,334,056 B1 12/2001 Holmes et al.
6,338,140 B1 1/2002 Owens et al.
6,349,134 B1 2/2002 Katz
6,385,729 B1 5/2002 DiGiorgio et al.
6,387,729 B2 5/2002 Eng et al.
6,393,468 B1 5/2002 McGee
6,400,726 B1 6/2002 Piret et al.
6,466,780 B1 10/2002 Geiselman et al.
6,535,726 B1 3/2003 Johnson
6,584,309 B1 6/2003 Whigham
6,687,241 B1 2/2004 Goss
6,707,915 B1 3/2004 Jobst et al.
6,731,731 B1 5/2004 Ueshima
6,934,858 B2 * 8/2005 Woodhill 726/5
6,993,658 B1 1/2006 Engberg et al.
6,993,663 B1 1/2006 Paya et al.
7,007,301 B2 2/2006 Crosbie et al.
7,024,688 B1 4/2006 Faccin et al.
7,025,179 B2 4/2006 Shih
7,028,179 B2 4/2006 Anderson et al.
7,058,796 B2 6/2006 Lynn et al.
7,058,968 B2 6/2006 Rowland et al.
7,100,204 B1 8/2006 Myllymaki et al.
7,133,662 B2 11/2006 Bravo et al.
7,142,840 B1 11/2006 Geddes et al.
7,221,949 B2 5/2007 Clough
7,290,278 B2 10/2007 Cahill et al.
7,317,693 B1 1/2008 Roesch et al.
7,324,976 B2 1/2008 Gupta et al.
7,337,431 B1 2/2008 Barnes et al.
7,357,310 B2 4/2008 Calabrese et al.
7,360,248 B1 4/2008 Kanevsky et al.
7,376,431 B2 5/2008 Niedermeyer
7,379,921 B1 5/2008 Kiliccote
7,380,708 B1 6/2008 Kiliccote
7,447,494 B2 11/2008 Law et al.
7,480,805 B1 1/2009 Gnech et al.
7,491,308 B2 2/2009 Talieh et al.
7,519,989 B2 4/2009 Lin et al.
7,533,414 B1 5/2009 Reed et al.
7,536,634 B2 5/2009 Green et al.
7,540,022 B2 5/2009 Barrari et al.
7,594,270 B2 9/2009 Church et al.
7,600,676 B1 10/2009 Rados et al.
7,609,625 B2 10/2009 Wei et al.
7,623,458 B2 11/2009 Ayyagari et al.
7,624,447 B1 11/2009 Horowitz et al.
7,665,128 B2 2/2010 Yang
7,673,334 B2 3/2010 Takemori et al.
7,715,823 B2 5/2010 Bravo et al.
7,716,742 B1 5/2010 Roesch et al.
7,757,285 B2 7/2010 Kubota
7,765,584 B2 7/2010 Roskind
7,779,465 B2 8/2010 Baker et al.
7,823,199 B1 10/2010 Rathi et al.
7,840,993 B2 11/2010 Ganesan et al.
7,845,004 B2 11/2010 Bardsley et al.
7,886,346 B2 2/2011 Sandhu et al.
7,926,108 B2 4/2011 Rand et al.
7,930,540 B2 4/2011 Ahuja et al.
7,954,150 B2 5/2011 Croft et al.
7,975,293 B2 7/2011 Yoshida et al.
8,019,995 B2 9/2011 van Bemmel
8,024,567 B2 9/2011 Han
8,050,658 B2 11/2011 Hong
8,060,915 B2 11/2011 Voice et al.
8,136,150 B2 3/2012 Hayler et al.
8,150,370 B2 4/2012 Dempo et al.
8,151,327 B2 4/2012 Eisen
8,181,248 B2 5/2012 Oh et al.
8,201,217 B1 6/2012 Begen et al.
8,254,542 B2 8/2012 Frederick
8,281,375 B2 10/2012 von Krogh
8,285,639 B2 10/2012 Eden et al.
8,296,823 B2 10/2012 Schubert
8,301,877 B2 10/2012 Grajek et al.
8,302,180 B1 10/2012 Gudov et al.
8,302,187 B1 10/2012 Gupta et al.
2001/0054155 A1 12/2001 Hagan et al.
2002/0069165 A1 6/2002 O'Neil
2002/0091931 A1 7/2002 Quick et al.
2002/0095588 A1 7/2002 Shigematsu et al.
2002/0178070 A1 11/2002 Leveridge
2002/0178370 A1 11/2002 Gurevich et al.
2003/0014315 A1 1/2003 Jaalinoja et al.
2003/0154382 A1 8/2003 Vicard
2003/0172272 A1 9/2003 Ehlers et al.
2004/0148520 A1 7/2004 Talpade et al.
2004/0152446 A1 8/2004 Saunders et al.
2004/0198329 A1 10/2004 Vasa
2004/0243856 A1 12/2004 Shatford
2005/0015624 A1 1/2005 Ginter et al.
2005/0018618 A1 1/2005 Mualem et al.
2005/0022020 A1 1/2005 Fremberg
2005/0060535 A1 3/2005 Bartas
2005/0075070 A1 4/2005 Crilly, Jr.
2005/0182958 A1 8/2005 Pham et al.
2005/0187934 A1 8/2005 Motsinger et al.
2005/0188423 A1 8/2005 Motsinger et al.
2005/0210251 A1 9/2005 Nyberg et al.
2006/0021031 A1 1/2006 Leahy et al.
2006/0036690 A1 2/2006 O'Neil
2006/0094403 A1 5/2006 Norefors et al.
2006/0095955 A1 5/2006 Vong
2006/0179304 A1 8/2006 Han
2006/0248021 A1 * 11/2006 Jain et al. 705/75
2006/0288411 A1 12/2006 Garg et al.
2007/0015492 A1 1/2007 Bravo et al.
2007/0067828 A1 3/2007 Bychkov
2007/0083606 A1 4/2007 Malik et al.
2007/0084913 A1 4/2007 Weston
2007/0107050 A1 5/2007 Selvarajan
2007/0136573 A1 6/2007 Steinberg
2007/0136808 A1 6/2007 Xiong
2007/0143851 A1 6/2007 Nocodemus et al.
2007/0186099 A1 8/2007 Beck et al.
2007/0220275 A1 9/2007 Heitzeberg et al.
2007/0234426 A1 10/2007 Khanolkar et al.
2007/0261112 A1 11/2007 Todd et al.
2007/0266257 A1 11/2007 Camaisa et al.
2008/0028447 A1 1/2008 O'Malley et al.
2008/0172730 A1 7/2008 Sandhu et al.
2008/0181380 A1 7/2008 Gustave et al.
2008/0189776 A1 8/2008 Constable
2008/0209275 A1 8/2008 Kwan et al.
2008/0270301 A1 10/2008 Jones et al.
2008/0318548 A1 12/2008 Bravo et al.
2009/0037329 A1 2/2009 Coppinger et al.
2009/0077637 A1 3/2009 Santos et al.
2009/0094682 A1 4/2009 Sage et al.
2009/0104889 A1 4/2009 Lotvonen et al.
2009/0106138 A1 4/2009 Smith et al.
2009/0300738 A1 12/2009 Dewe et al.
2010/0024017 A1 1/2010 Ashfield et al.
2010/0051686 A1 3/2010 Obi
2010/0095351 A1 4/2010 Liu et al.
2010/0269162 A1 10/2010 Bravo et al.
2011/0039237 A1 2/2011 Skare
2011/0138483 A1 6/2011 Bravo et al.
2011/0154459 A1 6/2011 Kuang et al.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2011/0197070	A1	8/2011	Mizrah	
2011/0225647	A1	9/2011	Dilley et al.	
2011/0277024	A1	11/2011	Begley et al.	
2011/0289576	A1	11/2011	Cheng	
2011/0307366	A1*	12/2011	Ahuja et al.	705/37
2012/0011066	A1	1/2012	Telle et al.	
2012/0149334	A1	6/2012	Zhang et al.	
2012/0180097	A1*	7/2012	Addington et al.	725/109
2012/0204241	A1	8/2012	Varsavsky Waisman-Diamond et al.	
2012/0264405	A1	10/2012	Bravo et al.	
2012/0272331	A1	10/2012	Lemaster et al.	
2013/0007859	A1	1/2013	Bravo et al.	
2014/0011561	A1*	1/2014	Lutnick et al.	463/17
2014/0016634	A1*	1/2014	Khan et al.	370/352
2014/0033279	A1*	1/2014	Nimashakavi et al.	726/4

FOREIGN PATENT DOCUMENTS

GB	2456509	A	7/2009
JP	10334048		12/1998
JP	10334048	A	12/1998
JP	10341224	A	12/1998
JP	2001111545		4/2001
WO	0109808	A1	2/2001
WO	2004079499	A2	9/2004
WO	2006103387	A1	10/2006
WO	2008147353	A1	12/2008

OTHER PUBLICATIONS

Almeida, U.S. Appl. No. 12/630,875, Office Action, Apr. 17, 2013, 40 pages.

Lakhia, U.S. Appl. No. 11/753,673, Notice of Allowance & Fees Due, dated May 10, 2013, 28 pages.

Vaughan, U.S. Appl. No. 12/423,928, Notice of Allowance & Fees Due, Jul. 11, 2013, 25 pages.

Alicherry et al.; "DoubleCheck: Multi-Path Verification Against Man-in-the-Middle Attacks", ISCC IEEE Symposium on, Jul. 5-8, 2009, pp. 557-563.

Kooi et al.; "VoIP Interception in PcP SIP Environment", ICCAE 2nd International Conference on, vol. 1, Feb. 26-28, 2010, pp. 331-334.

Kopsidas et al.; "Voice Interactive Personalized Security (VoIPSEC) Protocol . . . and Biometric Verification", HOTWEB 1st IEEE Workshop on, Nov. 13-14, 2006, pp. 1-10.

Leung Chun-Ming; "Depress Phishing by CAPTCHA with OTP", ASID 3rd International Conference on, Aug. 20-22, 2009, pp. 187-192.

Kumaraguru et al., "Getting Users to Pay Attention to Antiphishing Education: Evaluation of Retention and Transfer", APWG eCrime Researchers Summit, Oct. 4-5, 2007, pp. 70-81, Pittsburgh, PA.

Adida, "Beamauth: Two-Factor Web Authentication with a Bookmark", CCS, Oct. 29-Nov. 2, 2007, pp. 48-57, Alexandria, VA.

Nassar et al., "Holistic VoIP Intrusion Detection and Prevention System", IPTCOMM, 2007, pp. 1-9, New York.

Stoll et al., "Sesame: Informing User Security Decisions with System Visualization", CHI, Apr. 5-10, 2008, pp. 1045-1053, Florience Italy.

"Prevent Online Banking Fraud", Dec. 7, 2010, http://www.phonefactor.com/products/transaction-verification, 1 pages.

Vaughan, U.S. Appl. No. 13/613,502, Office Action Communication, Jul. 18, 2013, 54 pages.

Gee, U.S. Appl. No. 13/084,823, Office Action Communication, Jul. 19, 2013, 24 pages.

Almeida, U.S. Appl. No. 12/630,875, Office Action Communication, Aug. 7, 2013, 15 pages.

U.S. Appl. No. 12/630,875, Notice of allowance and Fee(s) Due dated Nov. 18, 2013, IBMC-0353, 19 pages.

Ma et al., "Beyond Blacklists: Learning to Detect Malicious Web Sites from Suspicious URLs", KDD '09, Jul. 28-Jul. 1, 2009, pp. 1245-1253.

Lakhia, U.S. Appl. No. 13/432,956, Notice of Allowance & Fees Due, Apr. 15, 2013, 27 pages.

Lakhia, U.S. Appl. No. 11/753,673, Office Action 1, IBMC-0208, 13 pages, Apr. 15, 2010.

Lakhia, U.S. Appl. No. 11/753,673, Final Office Action 1, IBMC-0208, 13 pages, Oct. 8, 2010.

Lakhia, U.S. Appl. No. 11/753,673, Office Action 2, IBMC-0208, 15 pages, Dec. 22, 2011.

Lakhia, U.S. Appl. No. 11/753,673, Notice of Allowance 1, IBMC-0208, 11 pages, Jun. 18, 2012.

Lakhia, U.S. Appl. No. 11/753,673, Notice of Allowance 2, IBMC-0208, 14 pages, Jan. 8, 2013.

Megeed, U.S. Appl. No. 12/423,928, Office Action 1, IBMC-0326, 21 pages, Aug. 25, 2011.

Megeed, U.S. Appl. No. 12/423,928, Final Office Action 1, IBMC-0326, 20 pages, Nov. 10, 2011.

Megeed, U.S. Appl. No. 12/423,928, Office Action 2, IBMC-0326, 20 pages, Jun. 8, 2012.

Megeed, U.S. Appl. No. 12/423,928, Notice of Allowance 1, IBMC-0326, 10 pages, Sep. 25, 2012.

Megeed, U.S. Appl. No. 12/423,928, Notice of Allowance 2, IBMC-0326, 19 pages, Dec. 4, 2012.

Bibbee, U.S. Appl. No. 11/765,193, Office Action 1, 15 pages, Feb. 18, 2010.

Bibbee, U.S. Appl. No. 11/765,193, Office Action 2, 14 pages, Nov. 29, 2010.

Bibbee, U.S. Appl. No. 11/765,193, Office Action 3, 18 pages, Sep. 19, 2011.

Bibbee, U.S. Appl. No. 11/765,193, Final Office Action 1, 15 pages, Jul. 30, 2010.

Bibbee, U.S. Appl. No. 11/765,193, Final Office Action 2, 17 pages, May 12, 2011.

Bibbee, U.S. Appl. No. 11/765,193, Final Office Action 3, 18 pages, Apr. 16, 2012.

Tran, U.S. Appl. No. 11/524,340, Office Action, 9 pages, Jul. 29, 2009.

Tran, U.S. Appl. No. 11/524,340, Office Action, 19 pages, Oct. 31, 2008.

Tran, U.S. Appl. No. 11/524,340, Notice of Allowance, 11 pages, Dec. 29, 2009.

Tran, U.S. Appl. No. 11/524,340, Office Action, 7 pages, Apr. 29, 2009.

Tran, U.S. Appl. No. 11/524,340, Office Action, 22 pages, May 27, 2008.

Juels, "Strengthening EPC Tags Against Cloning", WISE '05, Sep. 2, 2005, pp. 67-75.

Almeida, U.S. Appl. No. 12/630,875, Office Action, Mar. 1, 2012, 17 pages.

Almeida, U.S. Appl. No. 12/630,875, Office Action, Aug. 30, 2012, 14 pages.

Almeida, U.S. Appl. No. 12/630,875, Notice of Allowance, Dec. 20, 2012, 7 pages.

Stoll et al., "Sesame: Informing User Security Decisions with System Visualization", CHI 2008 Proceedings, Am I Safe, Apr. 5-10, 2008, Florence, Italy, pp. 1045-1054.

Lee et al., "A Resilient Packet-Forwarding Scheme against Maliciously Packet-Dropping Nodes in Sensor Networks" SASN '06, Oct. 30, 2005, ACM 1-59593-544-J/06/0010, pp. 59-69.

Deng et al., "Defending Against Redirect Attacks in Mobile IP", CCS '02, Nov. 18-22, 2002, ACM 1-58113-612-9/02/0011, pp. 59-67.

Kaafar et al., "Real attacks on virtual networks: Vivaldi out of tune", SIGCOMM '06 Workshops, Sep. 11-15, 2006, ACM 1-59593-417-0/06/0009, pp. 139-146.

Geneiatakis et al., "Survey of Security Vulnerabilities in Session Initiation Protocol", 3rd Quarter 2006, vol. 8, No. 3, IEEE Communications Surveys & Tutorials, pp. 68-81.

Gee, U.S. Appl. No. 13/084,823, Office Action, IBMC-0395, Mar. 11, 2013, 8 pages.

Bonzo, U.S. Appl. No. 11/776,619, Office Action, Sep. 30, 2009, 12 pages.

Bonzo, U.S. Appl. No. 11/776,619, Notice of Allowance, Apr. 29, 2010, 10 pages.

(56) **References Cited**

OTHER PUBLICATIONS

Lakhia, U.S. Appl. No. 13/432,956, Office Action 1, IBMC-0208-CON, Feb. 14, 2013, 26 pages.
Viral, U.S. Appl. No. 11/753,673, Notice of Allowance, Aug. 21, 2012, 7 pages.
U.S. Appl. No. 13/084,826, Office Action dated Feb. 3, 2014, IBMC-0395, 12 pages.
U.S. Appl. No. 13/613,502, Notice of allowance and Fee(s) Due dated Jan. 27, 2014, IBMC-0326-CON, 14 pages.
U.S. Appl. No. 13/084,823, Notice of Allowance and Fees Due, May 1, 2014, 16 pages.

* cited by examiner

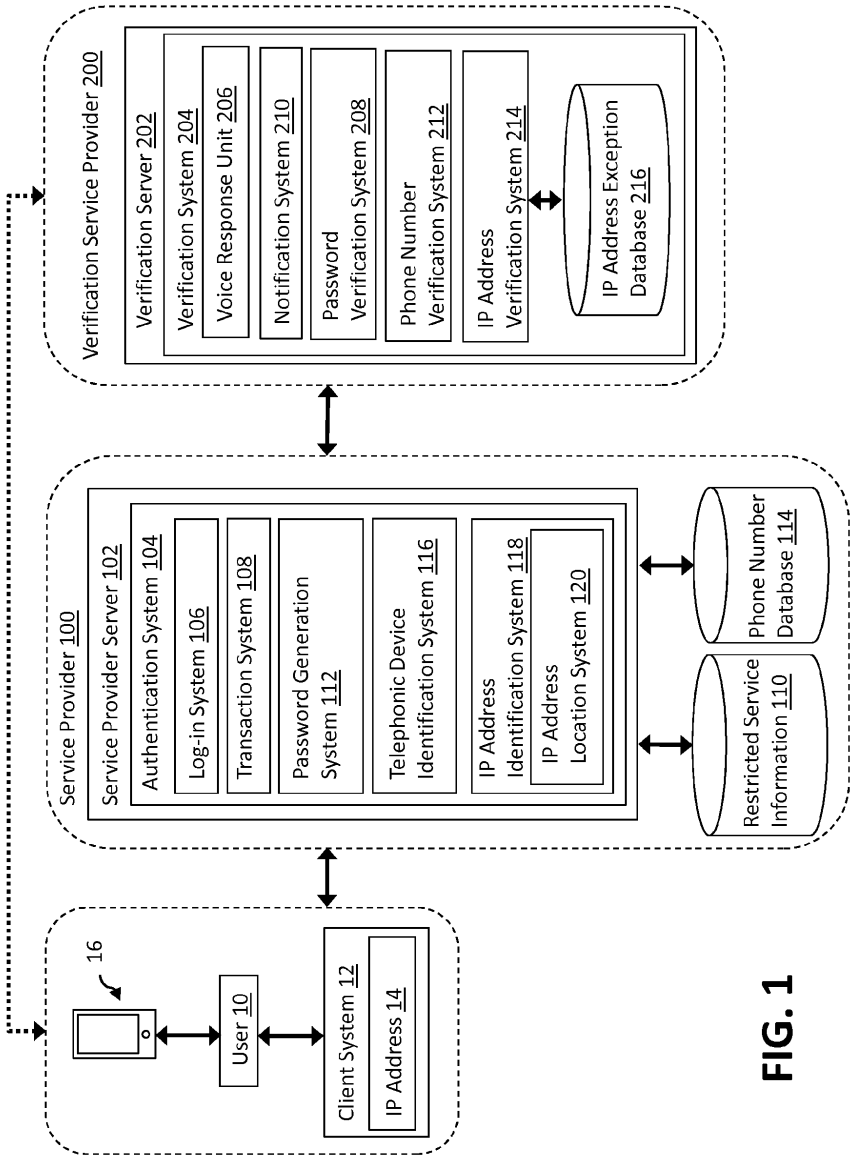

Verification Service Provider 200
Verification Server 202
Verification System 204
Voice Response Unit 206
Notification System 210
Password Verification System 208
Phone Number Verification System 212
IP Address Verification System 214
IP Address Exception Database 216
Service Provider 100
Service Provider Server 102
Authentication System 104
Log-in System 106
Transaction System 108
Password Generation System 112
Telephonic Device Identification System 116
IP Address Identification System 118
IP Address Location System 120
Phone Number Database 114
Restricted Service Information 110
16
User 10
Client System 12
IP Address 14

FIG. 1

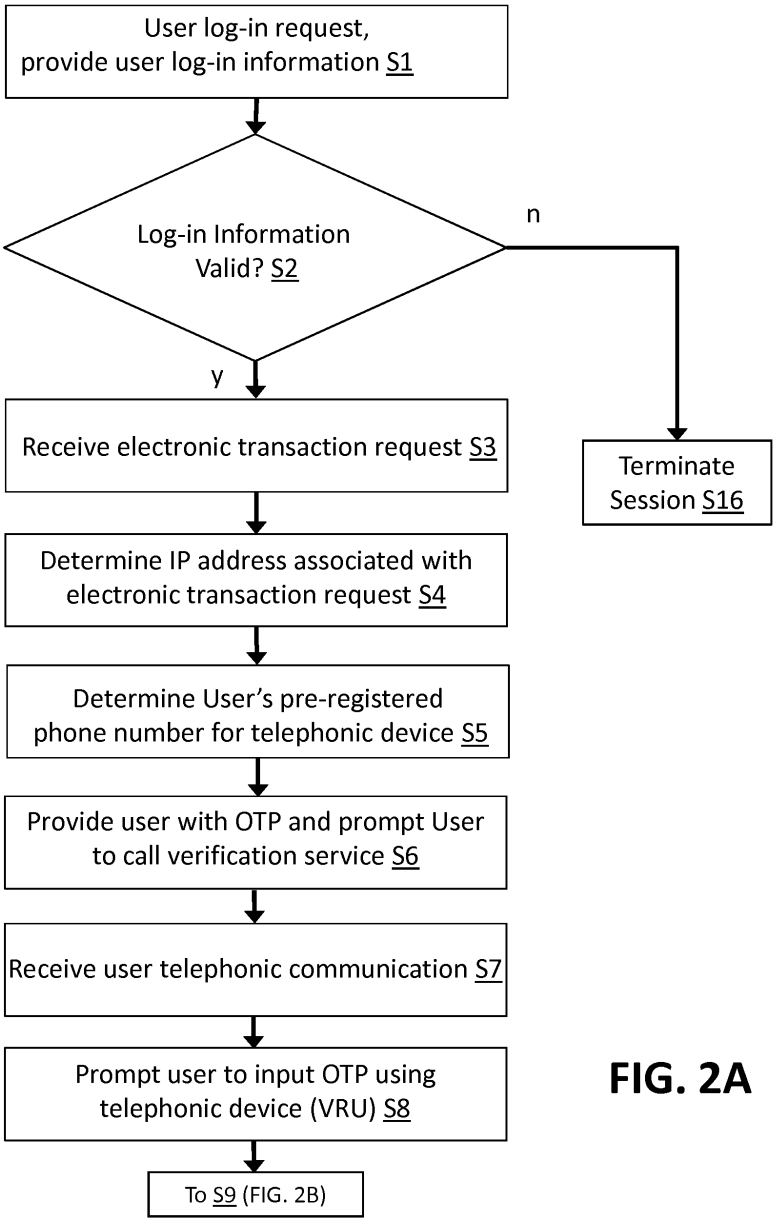

User log-in request, provide user log-in information S1
Log-in Information Valid? S2
n
y
Terminate Session S16
Receive electronic transaction request S3
Determine IP address associated with electronic transaction request S4
Determine User's pre-registered phone number for telephonic device S5
Provide user with OTP and prompt User to call verification service S6
Receive user telephonic communication S7
Prompt user to input OTP using telephonic device (VRU) S8
To S9 (FIG. 2B)

FIG. 2A

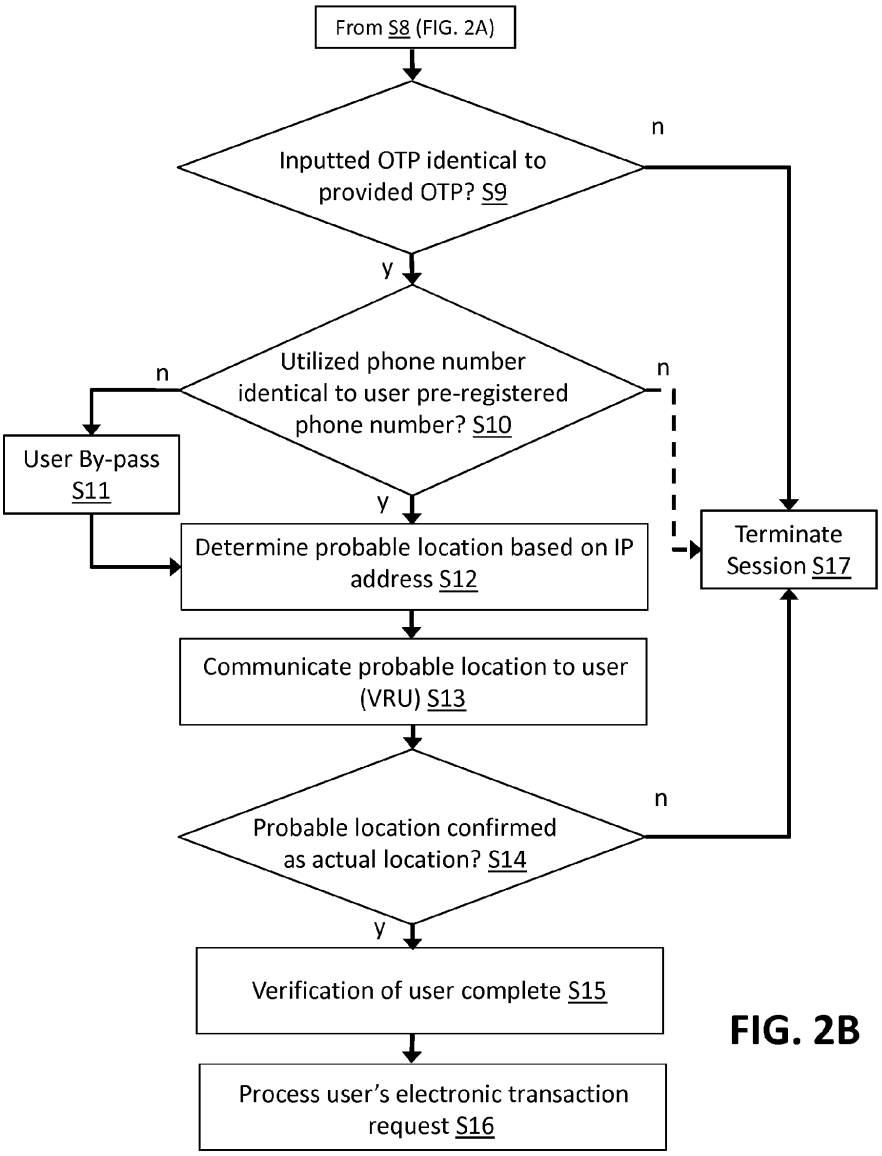

From S8 (FIG. 2A)
Inputted OTP identical to provided OTP? S9
n
y
Utilized phone number identical to user pre-registered phone number? S10
n
n
y
User By-pass S11
Determine probable location based on IP address S12
Terminate Session S17
Communicate probable location to user (VRU) S13
Probable location confirmed as actual location? S14
n
y
Verification of user complete S15
Process user's electronic transaction request S16

FIG. 2B

DETECTING MAN-IN-THE-MIDDLE ATTACKS IN ELECTRONIC TRANSACTIONS USING PROMPTS

BACKGROUND

1. Technical Field

The subject matter disclosed herein relates generally to a transaction authentication system. Specifically, the subject matter disclosed herein relates to detecting man-in-the-middle attacks in electronic transactions using prompts.

2. Related Art

Use of electronic media has quickly become the preferred means for a user to conduct electronic transactions. Users utilize transactions like, online-banking and Internet shopping every day, in order to avoid having to visit a physical location to conduct these transactions. However, these electronic transactions come with a heightened risk, as electronic transactions usually involve proprietary or sensitive information (e.g., bank account numbers, credit card numbers, etc.), collectively known as restricted user information. If a third party were to obtain this restricted user information, that party would be able to conduct transactions, which would typically be restricted, to simultaneously benefit the third party while harming the true owner of that restricted user information.

Third parties may obtain such information by conducting what is called a "man-in-the-middle" attack on an electronic transaction. A man-in-the-middle attack occurs when an third party computer system interposes itself between a user's computer system, used to conduct an electronic transaction, and a service provider's computer system, for providing the service involved in the electronic transaction. While interposed between the user and service provider systems, the third party computer system intercepts the restricted user information and electronic transaction information from the user's computer system, forwards along the gathered information to obtain access to the service providers system using the restricted user information, and conducts a distinct electronic transaction to benefit the third party and not the user. To keep the user from noticing the user's transaction has been interrupted by a man-in-the-middle attack, the third party system sends the user a fraudulent confirmation message or webpage confirming the user's electronic transaction information, when, in fact, a distinct electronic transaction has taken place. When a man-in-the-middle attack occurs, the user has no way of knowing until after the fraudulent electronic transaction has taken place, and the user desired electronic transaction has been discarded by the third party system.

BRIEF SUMMARY

A transactional authentication system is disclosed. One embodiment includes a method for authenticating an electronic transaction. The method includes: receiving an electronic transaction request from a user, the electronic transaction request originating at a client system; determining an IP address associated with the client system from which the received electronic transaction request originates; providing the user with a one time password associated with the electronic transaction request; receiving a telephonic communication from a telephonic device associated with the user; prompting the user, via a voice response unit, to input the password using the telephonic device; authenticating the user based on a comparison of the inputted password and the provided one time password; determining a probable location of the user based on the determined IP address of the client system; communicating to the user, via the voice response unit, the probable location of the user based on the determined IP address associated with the client system; and prompting the user to confirm the probable location of the user based on the IP address associated with the client system.

A first aspect of the invention includes a method for authenticating an electronic transaction. The method includes: receiving an electronic transaction request from a user, the electronic transaction request originating at a client system; determining an IP address associated with the client system from which the received electronic transaction request originates; providing the user with a one time password associated with the electronic transaction request; receiving a telephonic communication from a telephonic device associated with the user; prompting the user, via a voice response unit, to input the password using the telephonic device; authenticating the user based on a comparison of the inputted password and the provided one time password; determining a probable location of the user based on the determined IP address of the client system; communicating to the user, via the voice response unit, the probable location of the user based on the determined IP address associated with the client system; and prompting the user to confirm the probable location of the user based on the IP address associated with the client system.

A second aspect of the invention includes a computer system having: at least one computing device configured to authenticate a transaction by performing actions including: receiving an electronic transaction request from a user, the electronic transaction request originating at a client system; determining an IP address associated with the client system from which the received electronic transaction request originates; providing the user with a one time password associated with the electronic transaction request; receiving a telephonic communication from a telephonic device associated with the user; prompting the user, via a voice response unit, to input the password using the telephonic device; authenticating the user based on a comparison of the inputted password and the provided one time password; determining a probable location of the user based on the determined IP address of the client system; communicating to the user, via the voice response unit, the probable location of the user based on the determined IP address associated with the client system; and prompting the user to confirm the probable location of the user based on the IP address associated with the client system.

A third aspect of the invention includes a computer program product for authenticating an electronic transaction, the computer program product comprising a computer readable storage medium having program code embodied therewith, the program code executable by at least one computer system to perform a method. The method includes: receiving an electronic transaction request from a user, the electronic transaction request originating at a client system; determining an IP address associated with the client system from which the received electronic transaction request originates; providing the user with a one time password associated with the electronic transaction request; receiving a telephonic communication from a telephonic device associated with the user; prompting the user, via a voice response unit, to input the password using the telephonic device; authenticating the user based on a comparison of the inputted password and the provided one time password; determining a probable location of the user based on the determined IP address of the client system; communicating to the user, via the voice response unit, the probable location of the user based on the determined IP address associated with the client system; and prompting the user to confirm the probable location of the user based on the IP address associated with the client system.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other features of this invention will be more readily understood from the following detailed description of the various aspects of the invention taken in conjunction with the accompanying drawings that depict various embodiments of the invention, in which:

FIG. **1** shows a schematic depiction of a transactional authentication environment according to embodiments of the invention.

FIGS. **2**A-**2**B show a flow diagram illustrating a method according to embodiments of the invention.

It is noted that the drawings of the invention are not necessarily to scale. The drawings are intended to depict only typical aspects of the invention, and therefore should not be considered as limiting the scope of the invention. In the drawings, like numbering represents like elements between the drawings.

DETAILED DESCRIPTION

As described herein, aspects of the invention relate to a transaction authentication system. Specifically, as described herein, aspects of the invention relate to a system for authenticating transactions by verifying a user's transactional request location.

The described embodiments provide superior security for electronic transactions which involves a user's restricted information. More specifically, the authentication of the electronic transaction involving a service provider in the embodiments as described herein provides greater security than conventional authentication systems. In some authentication embodiments, such as that described in US 2008/0318548, published on Dec. 25, 2008, entitled "Method and System for Strong Authentication and Defense against Man-in-the-Middle Attacks," the contents of which are hereby incorporated by reference, the location of the user's computer IP address are examined by the restricted item provider to determine if the two are proximately located. The service provider, as described herein, and the restricted item provider, as described by the incorporated reference, may be any entity that provides goods and/or services, and controls access to restricted or user sensitive information, e.g., bank, business, website, server, etc.

Turning to FIG. **1**, a schematic depiction of a transactional authentication environment according to embodiments of the invention is provided. The transactional authentication environment includes a service provider **100** and a third party verification service provider **200**. As discussed above, service provider **100** may include any entity that provides goods and/or services, and controls access to restricted or user-sensitive information. User **10** may access the goods and/or services of service provider **100** using a client system **12**. More specifically, user **10** may utilize client system **12** to access the goods and/or services of service provider **100** by communicating with a service provider server **102** of service provider **100** over a network. Client system **12** may include any device, software or system, such as a World Wide Web (web) browser included on a personal computer system, a handheld device, a smart-phone, an ATM machine, etc., which may include a unique network identifier. In an embodiment, as shown in FIG. **1**, the unique network identifier of client system **12** may include an Internet Protocol (IP) address **14**. Service provider server **102** may provide user **10** with an interactive website or any other conventional electronic medium in which user **10** may utilize client system **12** to conduct electronic transactions offered by service provider **100**.

For example, service provider **100** may be a bank, and service provider server **102** may provide client system **12** with a banking website capable of processing banking transactions. Specifically in the example, service provider server **102** may provider client system **12** with a website, which may allow user **10**, a member of the bank associated with service provider **100**, to conduct electronic banking transactions using client system **12**.

With respect to the authentication environment, authentication of user's **10** electronic transaction request of service provider **100** is provided below. In an embodiment, as shown in FIG. **1**, service provider server **102** may include an authentication system **104** which may be implemented as any combination of hardware and software (i.e., a computer system and/or a program product). Authentication system **104** may further include sub-components for, at least in part, authenticating an electronic transaction request made by user **10**. As shown in FIG. **1**, authentication system **104** may include a log-in system **106**. As a result of user **10** attempting to access service provider server **102** via client system **12**, log-in system **106** may provide user **10** with a log-in mechanism to verify the specific user **10** attempting to access service provider server **102**. More specifically, log-in system **106** may prompt user **10** to enter user **10** specific log-in information, e.g., user ID, user name, user e-mail, user password, etc., to verify the specific user **10** attempting to access service provider server **102**.

In continuing the example embodiment above, user **10** may direct client system **12** to a bank website (e.g., service provider server **102**) in order to conduct electronic banking transactions. After directing client system **12** to the bank website, log-in system **106** of authentication system **104** may prompt user **10** to enter a user ID and associated password to verify that user **10** is a member of the bank (e.g., service provider **100**).

Authentication system **104** may also include a transaction system **108** which may collect information relating to electronic transaction requests made by user **10**. More specifically, transaction system **108** may be configured to receive the electronic transaction requests made by user **10** requesting to access restricted service information **110**. Restricted service information **110** may include any type of information for which authorization is required.

Continuing the example embodiment, after user **10** has successfully logged in to service provider server **102**, user **10**, via client system **12**, may send an electronic transaction request to service provider server **102**. For example, user **10** may send an electronic transaction requesting to transfer $500 USD from user's **10** checking account to user's **10** savings account, both of which may be accounts held by the bank (e.g., service provider **100**). The account numbers associated with each of user's **10** accounts are restricted service information **110**, and may be required to successfully process the electronic transaction request. Furthermore, the account numbers (e.g., restricted service information **110**) may require further authorization before any transfer of user's **10** funds may be made.

Authentication system **104** may also include a password generation system **112**. Password generation system **112** may be configured to generate a password for user **10** for, in part, authenticating user **10** electronic transaction request involving service provider **100**. More specifically, password generation system **112** may generated a one-time password (OTP), and may relay the OTP to user **10** via service provider

server **102**. Additionally, service provider server **102** may prompt user **10** to contact and provide third party verification service **200** with the OTP generated by password generation system **112**. In an embodiment, service provider server **102** may send the OTP to user **10** via client system **12**. In an alternative embodiment, service provider server **102** may send the OTP to a telephonic device **16** unique to user **10**. Telephonic device **16** may include, for example, any now known or later developed mobile device or local area network (LAN) telephone capable of telephonic communication. In an embodiment, telephonic device **16** associated with user **10** may include a phone number pre-registered with service provider **100**, and may be stored in a phone number database **114** in communication with service provider server **102**. More specifically, a phone number unique to telephonic device **16** may be stored in phone number database **114**, and may be used, in part, for authentication of user's **10** electronic transaction request, as discussed below. In an alternative embodiment, the pre-registered phone number of telephonic device **16** may be registered with third party verification service provider **200** or any other third party service provider used in the authentication process of the embodiments described herein.

In the example, after user **10** submits an electronic transaction request to service provider server **102** via client system **12**, and authentication system **104** recognizes the electronic transaction request requires further authentication, password generation system **112** may generate a multi-digit OTP ("0123456789") associated with user's **10** electronic transaction request of transferring $500 between accounts. The OTP generated by password generation system **112** may be provided to user **10** via service provider server's **102** banking website that is displayed on client system **12**. Along with the OTP password generated by password generation system **112**, service provider server **102** may prompt user **10** to call third party verification service provider **200** using telephonic device **16**, and enter the OTP using telephonic device **16** when prompted.

In the embodiment, as shown in FIG. **1**, authentication system **104** may also include a telephonic device identification system **116**. Telephonic device identification system **116** may be configured to determine the pre-registered phone number of telephonic device **16** associated with user **10**. More specifically, telephonic device identification system **116** may obtain the log-in information to identify specific user **10**, and obtain the pre-registered phone number associated with user's **10** telephonic device **16** from phone number database **114**. Telephonic device identification system **116** may also be configured to provide third party verification service provider **200** with the pre-registered phone number stored in phone number database **114** for, in part, authenticating user's **10** electronic transaction request.

Continuing the example, after user **10** receives the OTP generated by password generation system **112**, telephonic device identification system **116** may determine the pre-registered phone number of telephonic device **16** that may be associated with user **10**. That is, telephonic device identification system **116** may utilize user's **10** specific log-in information and obtain the pre-registered phone number of telephonic device **16** associated with user **10**. Specifically, telephonic device identification system **116** may determine that user's **10** pre-registered phone number is "555-555-5555." Once telephonic device identification system **116** obtains user's **10** pre-registered phone number for telephonic device **16**, telephonic device identification system **116** may send the user's **10** pre-registered phone number to third party verification service provider **200** using service provider server **102**.

Further in an embodiment, as shown in FIG. **1**, Authentication system **104** may include an IP address identification system **118**. IP address identification system **118** may be configured to determine IP address **14** associated with client system **12** from which the electronic transaction request may originate. More specifically, IP address identification system **118** may obtain user's **10** electronic transaction request information which may include IP address **14** associated with client system **12** from which the electronic transaction request originated. IP address identification system **118** may include an IP address location system **120** which may take IP address **14** associated with client system **12** from which user's **10** electronic transaction request originated, and may determine a probable geographic location of client system **12**. Systems for determining a probable geographic location of client system **12** based on IP address **14**, such as IP address location system **120**, are readily known in the art (e.g., www-.geobytes.com/IPlocator.htm). Further explanation of this system is omitted for clarity. IP address identification system **118** may also provide third party verification service provider **200** with the probable geographic location of client system **12** determined by IP address location system **120**. The probable geographic location may be used, in part, to authentication the electronic transaction requested by user **10**. In an alternative embodiment, IP address location system **120**, or a system configured to perform similar functions, may be implemented by third party verification service provider **200**, rather than service provider **100**. More specifically, IP address identification system **118** of authentication system **104** may be configured to obtain IP address **14**, and a system of third party verification service provider **200** may be configured to obtain IP address **14** from authentication system **104** and determine a probable geographic location of client system **12** based on the obtained IP address **14**.

Continuing the example embodiment, IP address identification system **118** may determine IP address **14** associated with client system **12** from which the electronic transaction request originated. Specifically, IP address identification system **118** may determine IP address **14** is 12.34.567.89. IP address location system **120** may then take IP address **14** associated with client system **12** (e.g., IP address 12.34.567.89) and determine that client system's **12** probable geo-location is Washington, D.C. Utilizing service provider server **102**, IP address identification system **118** may then transfer the probable geographic location of client system **12** (e.g., Washington, D.C.) to third party verification service provider **200** for, in part, authentication of the electronic transaction request (e.g., $500 bank account transfer) from user **10**.

Although described in series above, it is understood that password generation system **112**, telephonic device identification system **116** and/or IP address identification system **118** may perform each of their respective processes in parallel. For example, password generation system **118** may generate a OTP unique to user's **10** electronic transaction request in parallel to IP address identification system **118** determining IP address **14** associated with client system **12**.

In an embodiment, as shown in FIG. **1**, user **10** may verify information relating to the electronic transaction request by communicating with a verification server **202** of third party verification service provider **200**. More specifically, user **10** may use telephonic device **16** to contact verification server **202** of third party verification service provider **200** to provide information (e.g., OTP, etc.) so service provider **100** may

successfully authenticate and process user's **10** electronic transaction request. Verification server **202** may be configured as any conventional server now know or later developed, capable of receiving information for a remote device (e.g., pre-registered telephonic device **16**, client system **12**, etc.) over a network.

As shown in FIG. **1**, verification server **202** may include a verification system **204** which may be implemented as any combination of hardware and software (i.e., a computer system and/or a program product). Similar to authentication system **104** as discussed above, verification system **204** may further include sub-components for, at least in part, verifying user **10** information so service provider **100** may authenticate an electronic transaction of user **10**. As shown in FIG. **1**, verification system **204** may include a voice response unit (VRU) **206**. In an embodiment, VRU **206** of verification system **204** may be configured to prompt user **10** to input the OTP using telephonic device **16** after user **10** calls third party verification service provider **200**. More specifically, VRU **206** may ask user **10**, using computer simulated speech or a recording, to input the OTP generated by password generation system **112** of authentication system **104** using telephonic device **16**.

Continuing the example above, once user **10** receives the OTP, and is prompted to call the provided number for third party verification service provider **200** by the bank (e.g., service provider **100**), user **10** calls third party verification service provider **200** using his cell phone (e.g., telephonic device **16**). User **10** may then be connected to verification server **202**. Once connected, VRU **206** provides user **10** with, for example, the following simulated speech: "Please input the 10-digit one time password now." User **10** is able to hear this recording over user's **10** cell phone speaker and may then input the OTP using the number pad on his cell phone.

Verification system **204** may also include password processing system **208**. Password processing system **208** may compare the inputted OTP by user **10** with the OTP generated by password generation system **112**. More specifically, password processing system **208** may be configured to receive the OTP generated by password processing system **112** for user's **10** electronic transaction request and receive the OTP inputted by user **10** using telephonic device **16** to verify or authenticate that the inputted OTP is identical to the generated OTP. In an embodiment, if password processing system **208** verifies that user **10** inputted OTP is identical to the generated OTP, password processing system **208** may provide verification system **204** with instructions to continue the user **10** verification processes. In the alternative, if password processing system **208** determines that user **10** inputted OTP is not identical to the generated OTP, password processing system **208** may inform notification system **210** of verification system **204** that the inputted OTP is not identical to the generated OTP. Notification system **210** may be configured to provide service provider **100** with an "alert," which indicates that verification system **204** may have determined that user **10** may not be verified based on the information provided to third party verification service provider **200**. As a result of the alert from notification system **210**, user **10** may not be verified and user's **10** electronic transaction request may not be authenticated by servicer provider **100**. In an embodiment, notification system **210** may alert service provider **100** that user **10** inputted OTP was not identical to the generated OTP. In an alternative embodiment, and as discussed in more detail below, notification system **210** may alert service provider **100** that the phone number associated with the telephonic device utilized to call third party verification service provider **200** was not identical to the pre-registered phone number associated with telephonic device **16**. In another alternative embodiment, notification system **210** may alert service provider **100** that user **10** did not confirm that the probable geographic location of user **10** and/or client system **12** based on IP address **14** is substantially similar to the actual location of user **10** and/or client system **12**.

In the example, after user **10** enters the multi-digit password ("0123456789") associated with the electronic transaction request (e.g., $500 account transfer) with the bank (e.g., servicer provider **100**) using user's **10** cellphone (e.g., telephonic device **16**), password verification system **208** may verify that user **10** inputted password is identical to the password provided to verification system **208** by authentication system **104** of the bank. In the example, password verification system **208** obtains user's **10** inputted password of "0123456789." Additionally, password verification may previously obtain a generated password of "0123456789" from bank's (e.g., servicer provider **100**) authentication system **104**. Password verification system **208** may then compare user **10** inputted password to the generated password and determine whether the two passwords are identical. As a result, password verification system **208** may communicate with verification system **204** to continue user **10** verification process.

In the embodiment, as shown in FIG. **1**, verification system **204** may include a phone number verification system **212**. Phone number verification system **212** may be configured to verify the phone number associated with the telephonic device user **10** utilizes to contact third party verification service provider **200**. More specifically, phone number verification system **212** may obtain the pre-registered phone number associated with telephonic device **16** of user **10** from authentication **104**, and determine if the obtained phone number is identical to the phone number associated with the telephonic device user **10** utilized to call third party verification service provider **200**. In an embodiment, phone number verification system may obtain the phone number associated with the telephonic device used by user **10** by any now know or later developed process, e.g., caller ID, cell phone provider look-up, etc. In an embodiment, phone number verification system **212** may determine if the obtained pre-registered phone number is identical to the phone number associated with the telephonic device user **10** utilized to call third party verification service provider **200** after password verification system **208** determines user **10** inputted password is identical to the password generated by password generation system **112**. In an alternative embodiment, phone number verification system **212** may determine if the obtained pre-registered phone number is identical to the phone number associated with the telephonic device user **10** utilizes to call third party verification service provider **200** immediately after user **10** calls third party verification service provider **200**. In a further alternative embodiment, phone number verification system **212** may determine if the obtained pre-registered phone number is identical to the phone number associated with the telephonic device user **10** utilized to call third party verification service provider **200** in parallel to password verification system **208** determining that user **10** inputted password is identical to the password generated by password generation system **112**.

Similar to password verification system **208**, phone number verification system **212** may inform notification system **210** when the obtained pre-registered phone number associated with telephonic device **16** is not identical to the telephone number associated with the telephonic device utilized by user **10** to call third party verification servicer provider **200**. As discussed above, notification system **210** may be configured to provide service provider **100** with an "alert," which indi-

cates that verification system **204** may have determined that user **10** may not be verified based on the information provided to third party verification service provider **200**. As a result of the alert from notification system **210**, user **10** may not be verified and user's **10** electronic transaction request may not be authenticated by servicer provider **100**. In an alternative embodiment, verification system **204** may continue the verification of user **10** even though the obtained pre-registered phone number associated with telephonic device **16** is not identical to the telephone number associated with the telephonic device utilized by user **10** to call third party verification service provider **200**. More specifically, the alert from notification system **210**, may prompt verification system **204** to utilize VRU **206**, so user **10** may verify the pre-registered telephone number associated with user **10** is correct, or for user **10** to confirm the telephonic device utilized by user **10** has a number distinct from the pre-registered telephone number associated with user's **10** telephonic device **16**. As a result, user **10** may by-pass this step of verification performed by verification system **204** and may continue with the verification process to successfully complete the electronic transaction. In the embodiment, phone number verification system **212** may obtain the pre-registered phone number associated with user's **10** telephonic device **16** from authentication system **104** in a electronic message between the two servers over a network. More specifically, authentication system **104** may send the generated OTP, associated phone number and IP address **14** of client system **12** (discussed below), in a single message to verification system **204**. In an alternative embodiment, authentication system **104** may send each user's **10** information (e.g., pre-registered phone number, IP address **14**, generated OTP, etc.) in distinct messages to verification system **204**.

Continuing the example above, after user **10** has input an identical multi-digit password to the generated multi-digit password, phone number verification system **212** may determine if user's **10** cellphone includes a phone number identical to the pre-registered phone number associated with user's **10** telephonic device **16** stored on phone number database **114** of the bank's server (e.g., service provider server **102**). In the example, phone number verification system **212** may obtain the phone number associated with the cellphone user **10** utilizes to call third party verification service provider **200** using a caller ID system (not shown), to determine user's **10** cellphone number is "555-555-5555." Phone number verification system **212** may then compare the determined cellphone number to the previously received pre-registered phone number associated with telephonic device **16**, "555-555-5555." As a result of phone number verification system **212** determining the phone numbers are identical, phone number verification system **212** may communicate with verification system **204** to continue user **10** verification process.

In an embodiment, as best shown in FIG. **1**, verification system **204** may also include an IP address verification system **214**. IP address verification system **214** may be configured to provide the probable geographic location of client system **12** to user **10** from authentication system **104**. More specifically, IP address verification system **214** may obtain a probable geographic location of client system **12** from IP address location system **120** of authentication system **104** and provide the probably geographic location to VRU **206** to be audibly provided to user **10** via telephonic device **16**. In an embodiment, the computer simulated speech of VRU **206** may tell user **10** that client system **12** may be located in a probable geographic location, previously determined by IP address location system **120**. Additionally, VRU **206** may prompt user **10** to confirm the probable geographic location of user **10** and/or client system **12** is correct. If user **10** confirms the probable geographic location of user **10** and/or client system **12**, IP address verification system **214** may communicate with verification system **204** that probable geographic location of client system **12** has been verified and the verification process of user **10** may continue. However, if user **10** does not confirm the probable geographic location of user **10** and/or client system **12** is the actual (approximate) location of user **10** and/or client system **12**, IP address verification system **214** may inform notification system **210** of this denial in confirmation. As discussed above, as a result of the alert from notification system **210**, user **10** may not be verified and user's **10** electronic transaction request may not be authenticated by servicer provider **100**.

In an alternative embodiment, where client system **12** is a component of a computing network, IP address verification system **214** of verification system **204** may also include an IP address exception database **216**. IP address exception database **216** may include a list of pre-registered IP addresses which may be associated with proxies, or servers of the computing network which includes client system **12**. As a result of the use of the computing network, each client system **12** of computing network may include the IP address associated with the proxies or servers of computing network, and not necessarily the IP address associated with the actual location of client system **12**. In an embodiment, IP address verification system **214** may obtain IP address **14** from authentication system **104**, and may determine IP address **14** is included in the pre-registered IP addresses stored on IP address exception database **216**. As a result, the verification of the probable geographic location of user **10** and/or client system **12** performed by IP address verification system **214** may be skipped by third party verification service provider **200**. In an alternative embodiment, if user **10** is aware that IP address **14** of client system **12** may be directed to a probable location of a server or proxy of the computing network, and not the actual location of user **10** and/or client system **12**, user **10** may verify the probable geographic location of the server or proxy of computing network with verification system **204**. That is, user **10** may verify the probable location based on IP address **14**, even though user **10** may be located in an actual geographic location distinct from the probable geographic location.

In the example, after verification system **204** has verified both the user **10** inputted password and the phone number associated with the cellphone user **10** utilized to call third party verification service provider **200**, IP address verification system **214** may provide the probable location of user **10** and/or client system **12** (e.g, Washington, D.C.) to VRU **206** to audibly provide the probable location, so user **10** may confirm or deny the location. That is VRU **206** may provide user **10** with the following record: "Based on the detected IP address, you probable geographical location is Washington, D.C. Is this correct?" User **10** may speak his answer (e.g., yes or no) or may press a key using telephonic device **16** (e.g., cellphone) to confirm or deny that user **10** and/or client system **12** is actually locate in or near Washington, D.C. Once user **10** confirms the probable location, third party verification service provider **200** via verification server **202** may send a confirmation message to the bank (e.g., service provider **100**), indicating that user **10** has been verified, and user's **10** electronic transaction request may be authenticated and successfully processed. Transaction system **108** of Authentication system **104** may then process user's **10** electronic transaction request, or in the example, transfer $500 between user's **10** checking account and savings account, both held by the bank (e.g., service provider **100**).

Turning to FIGS. **2**A-**2**B, a flow diagram illustrating a method according to embodiments of the invention is disclosed. At **51**, a log-in request by user **10** is obtained (e.g., accessing service provider **100** website), where log-in information is provided by user **10**. At S**2**, it is determined if the log-in information provided by user **10** is valid. If no, the session is terminated S**17**. If yes, an electronic transaction request from user's **10** client system **12** is received, at S**3**. At S**4**, an IP address **14** associated with client system **12** from which the received electronic transaction request originated is determined. At S**5**, a pre-registered telephone number associated with telephonic device **16** of user **10** is determined. At S**6**, user **10** is provided with a OTP and is prompted to utilize telephonic device **16** to confirm the OTP with third party verification service provider **200**.

At S**7**, a third party verification service provider **200** receives a telephonic communication from telephonic device **16** associated with user **10**. At S**8**, VRU **206** of third party verification service provider **200** prompts user **10** to input the OTP using telephonic device **16**. At S**9**, it is determined if the inputted OTP is identical to the password provided to user **10** at S**6**. If no, the session is terminated S**17**. If yes, it is determined if the phone number associated with the telephonic device used by user **10** to call third party verification service provider **200** is identical to the pre-registered phone number associated with user's **10** telephonic device **16**, at S**10**. If no, user **10** may by-pass S**10** and proceed to S**12** by confirming the number of the pre-registered associated with user's **10** telephonic device **16**, or confirming user **10** would like to proceed in the verification process at S**11**. In an optional feature, if no at S**10**, the session is terminated S**17**. If yes at **510** or user **10** by-passes **510**, a probable location of user **10** and/or system client **12** is determined based on the determined IP address **14** of client system **12**, at S**12**. At S**13**, VRU **206** communicates the probable location of user **10** and/or client system **12** using telephonic device **16**. At S**14**, user **10** is prompted to confirm or deny the probable location of user **10** and/or client system **12** based on user's **10** or client system's **12** actual location. If denied, the session is terminated S**17**. If probable location is confirmed, third party verification service provider **200** verifies user **10** and notifies service provider **100** of user's **10** successful verification, at S**15**. At S**16**, service provider **100** authenticates and processes user's electronic transaction request.

Note that while the embodiments are described with reference to a telephonic device, the invention may be implemented with any device that has a unique discoverable identifier (e.g., phone number, email address, IP address, etc.) and can transmit a token to a third party verification service provider **200**.

Referring again to FIG. **1**, it is understood that each of the authentication system **104** and verification server **202** may be implemented using any type of computing device (i.e., computer system). Such a computing device generally includes a processor, input/output (I/O), memory, and bus. The processor may comprise a single processing unit, or be distributed across one or more processing units in one or more locations, e.g., on a client and server. Memory may comprise any known type of data storage, including magnetic media, optical media, random access memory (RAM), read-only memory (ROM), a data cache, a data object, etc. Moreover, memory may reside at a single physical location, comprising one or more types of data storage, or be distributed across a plurality of physical systems in various forms.

I/O may comprise any system for exchanging information to/from an external resource. External devices/resources may comprise any known type of external device, including a monitor/display, speakers, storage, another computer system, a hand-held device, keyboard, mouse, voice recognition system, speech output system, printer, facsimile, pager, etc. The bus provides a communication link between each of the components in the computing device and likewise may comprise any known type of transmission link, including electrical, optical, wireless, etc. Although not shown, additional components, such as cache memory, communication systems, system software, etc., may be incorporated.

Access may be provided over a network such as the Internet, a local area network (LAN), a wide area network (WAN), a virtual private network (VPN), etc. Communication could occur via a direct hardwired connection (e.g., serial port), or via an addressable connection that may utilize any combination of wireline and/or wireless transmission methods. Moreover, conventional network connectivity, such as Token Ring, Ethernet, WiFi or other conventional communications standards could be used. Still yet, connectivity could be provided by conventional TCP/IP sockets-based protocol. In this instance, an Internet service provider could be used to establish interconnectivity. Further, as indicated above, communication could occur in a client-server or server-server environment.

It should be appreciated that the teachings of the present invention could be offered as a business method on a subscription or fee basis. For example, a computer system comprising authentication system **104** and/or verification system **204** could be created, maintained and/or deployed by a service provider that offers the functions described herein for customers. That is, a service provider could offer to deploy or provide the ability to provide authentication as described above.

It is understood that in addition to being implemented as a system and method, the features may be provided as one or more program products stored on computer-readable storage mediums, which when run, enables one ore more computer systems to provide authentication as described. To this extent, the computer-readable storage medium may include program code, which implements the processes and systems described herein. It is understood that the term "computer-readable medium" comprises one or more of any type of physical embodiment of the program code. In particular, the computer-readable medium can comprise program code embodied on one or more portable storage articles of manufacture (e.g., a compact disc, a magnetic disk, a tape, etc.), on one or more data storage portions of a computing device, such as memory and/or a storage system.

As used herein, it is understood that the terms "program code" and "computer program code" are synonymous and mean any expression, in any language, code or notation, of a set of instructions that cause a computing device having an information processing capability to perform a particular function either directly or after any combination of the following: (a) conversion to another language, code or notation; (b) reproduction in a different material form; and/or (c) decompression. To this extent, program code can be embodied as one or more types of program products, such as an application/software program, component software/a library of functions, an operating system, a basic I/O system/driver for a particular computing and/or I/O device, and the like. Further, it is understood that terms such as "component" and "system" are synonymous as used herein and represent any combination of hardware and/or software capable of performing some function(s).

The block diagrams in the figures illustrate the architecture, functionality, and operation of possible implementations of systems, methods and computer program products accord-

ing to various embodiments of the present invention. In this regard, each block in the block diagrams may represent a module, segment, or portion of code, which comprises one or more executable instructions for implementing the specified logical function(s). It should also be noted that the functions noted in the blocks may occur out of the order noted in the figures. For example, two blocks shown in succession may, in fact, be run substantially concurrently, or the blocks may sometimes be run in the reverse order, depending upon the functionality involved. It will also be noted that each block of the block diagrams can be implemented by special purpose hardware-based systems which perform the specified functions or acts, or combinations of special purpose hardware and computer instructions.

Although specific embodiments have been illustrated and described herein, those of ordinary skill in the art appreciate that any arrangement which is calculated to achieve the same purpose may be substituted for the specific embodiments shown and that the invention has other applications in other environments. This application is intended to cover any adaptations or variations of the present invention. The following claims are in no way intended to limit the scope of the invention to the specific embodiments described herein.

What is claimed is:

1. A method of authenticating an electronic banking transaction, the method comprising:
- receiving an electronic banking transaction request from a user, the electronic transaction request originating at a client system;
- determining an Internet Protocol (IP) address associated with the client system from which the received electronic banking transaction request originates;
- providing the user with a one time password associated with the electronic banking transaction request;
- providing the user with a third party verification number associated with the electronic banking transaction request;
- receiving a telephonic communication to the third party verification number from a telephonic device associated with the user;
- prompting the user, via a voice response unit, to input the password using the telephonic device, the telephonic device having a user number;
- authenticating the user based on a comparison of the inputted password and the provided one time password and the user number where the authenticating is performed by a third-party service provider, wherein the third-party provider is not a participant in the electronic banking transaction;
- determining a probable location of the user based on the determined IP address of the client system;
- communicating to the user, via the voice response unit, the probable location of the user based on the determined IP address associated with the client system; and
- prompting the user to confirm the probable location of the user based on the IP address associated with the client system.

2. The method of claim **1**, further comprising processing the electronic banking transaction request for the user in response to the user confirming the probable location of the user based on the determined IP address is substantially similar to an actual location of the user.

3. The method of claim **1**, wherein the telephonic device includes at least one of a mobile device or a telephone.

4. The method of claim **1**, wherein the user number is pre-registered with the third-party service provider.

5. The method of claim **1**, further comprising cancelling the electronic banking transaction request in response to one of:
- receiving a telephonic communication from a distinct telephonic device that is not associated with the user,
- determining the inputted one time password differs from the provided one time password, or
- receiving a notification from the user indicating the user has cancelled the electronic banking transaction request in response to the probable location of the user differing from an actual location of the user.

6. The method of claim **1**, further comprising:
- determining if the IP address associated with the client system is included on a server proxies list; and
- performing one of:
  - excluding the user from confirming the probable location of the user based on the IP address in response to determining the IP address associated with the client system is included on the server proxies list, or
  - allowing the user to confirm the probable location of the user, independent of an actual location of the user, in response to determining the IP address associated with the client system is included on the server proxies list.

7. The method of claim **1**, wherein the determining of the probable location of the user based on the determined IP address associated with the client system is performed by a third party service provider who is not a participant in the electronic banking transaction.

8. A computer system comprising:
- at least one computing device configured to authenticate an electronic banking transaction by performing actions including:
  - receiving an electronic banking transaction request from a user, the electronic banking transaction request originating at a client system;
  - determining an Internet Protocol (IP) address associated with the client system from which the received electronic banking transaction request originates;
  - providing the user with a one time password associated with the electronic banking transaction request;
  - providing the user with a third party verification number associated with the electronic banking transaction request;
  - receiving a telephonic communication to the third party verification number from a telephonic device associated with the user;
  - prompting the user, via a voice response unit, to input the password using the telephonic device, the telephonic device having a user number;
  - authenticating the user based on a comparison of the inputted password and the provided password and the user number where the authenticating is performed by a third-party service provider, wherein the third-party provider is not a participant in the electronic banking transaction;
  - determining a probable location of the user based on the determined IP address of the client system;
  - communicating to the user, via the voice response unit, the probable location of the user based on the determined IP address associated with the client system; and
  - prompting the user to confirm the probable location of the user based on the IP address associated with the client system.

9. The computer system of claim **8**, further comprising:
- processing the electronic banking transaction request for the user in response to the user confirming the probable

location of the user based on the determined IP address is substantially similar to an actual location of the user.

10. The computer system of claim **8**, wherein the telephonic device includes at least one of a mobile device or a telephone.

11. The computer system of claim **8**, wherein the user number is pre-registered with the third-party service provider.

12. The computer system of claim **8**, further comprising:

cancelling the electronic banking transaction request in response to one of:

receiving a telephonic communication from a distinct telephonic device that is not associated with the user,

determining the inputted one time password differs from the provided one time password, or

receiving a notification from the user indicating the user has cancelled the electronic banking transaction request in response to the probable location of the user differing from an actual location of the user.

13. The computer system of claim **8**, further comprising:

determining if the IP address associated with the client system is included on a server proxies list; and

performing one of:

excluding the user from confirming the probable location of the user based on the IP address in response to determining the IP address associated with the client system is included on the server proxies list, or

allowing the user to confirm the probable location of the user, independent of an actual location of the user, in response to determining the IP address associated with the client system is included on the server proxies list.

14. The computer system of claim **8**, wherein the determining of the probable location of the user based on the determined IP address associated with the client system is performed by the third party service provider who is not a participant in the electronic banking transaction.

15. A computer program product for authenticating an electronic banking transaction, the computer program product comprising a non-transitory computer readable medium having program code embodied therewith, the program code executable by at least one computer system to perform a method comprising:

receiving an electronic banking transaction request from a user, the electronic transaction request originating at a client system;

determining an Internet Protocol (IP) address associated with the client system from which the received electronic banking transaction request originates;

providing the user with a one time password associated with the electronic banking transaction request;

providing the user with a third party verification number associated with the electronic banking transaction request;

receiving a telephonic communication to the third party verification number from a telephonic device associated with the user;

prompting the user, via a voice response unit, to input the password using the telephonic device, the telephonic device having a user number;

authenticating the user based on a comparison of the inputted password and the provided password and the user number where the authenticating is performed by a third-party service provider, wherein the third-party provider is not a participant in the electronic banking transaction;

determining a probable location of the user based on the determined IP address of the client system;

communicating to the user, via the voice response unit, the probable location of the user based on the determined IP address associated with the client system; and

prompting the user to confirm the probable location of the user based on the IP address associated with the client system.

16. The computer program product of claim **15** further comprises:

processing the electronic banking transaction request for the user in response to the user confirming the probable location of the user based on the determined IP address is substantially similar to an actual location of the user.

17. The computer program product of claim **15**, wherein the telephonic device includes at least one of a mobile device or a telephone.

18. The computer program product of claim **15**, wherein the user number is pre-registered with the third-party service provider.

19. The computer program product of claim **15** further comprises:

cancelling the electronic banking transaction request in response to one of:

receiving a telephonic communication from a distinct telephonic device that is not associated with the user,

determining the inputted one time password differs from the provided one time password, or

receiving a notification from the user indicating the user has cancelled the electronic banking transaction request in response to the probable location of the user differing from an actual location of the user.

20. The computer program product of claim **15** further comprises:

determining if the IP address associated with the client system is included on a server proxies list; and

performing one of:

excluding the user from confirming the probable location of the user based on the IP address in response to determining the IP address associated with the client system is included on the server proxies list, or

allowing the user to confirm the probable location of the user, independent of an actual location of the user, in response to determining the IP address associated with the client system is included on the server proxies list.

21. The computer program product of claim **15**, wherein the determining of the probable location of the user based on the determined IP address associated with the client system is performed by a third party service provider who is not a participant in the electronic banking transaction.

* * * * *

(12) **United States Patent**
Bravo et al.

(10) **Patent No.: US 10,027,770 B2**
(45) **Date of Patent: Jul. 17, 2018**

(54) **EXPECTED LOCATION-BASED ACCESS CONTROL**

(71) Applicant: **International Business Machines Corporation**, Armonk, NY (US)

(72) Inventors: **Jose Bravo**, Mamaroneck, NY (US); **Jeffery L. Crume**, Raleigh, NC (US)

(73) Assignee: **International Business Machines Corporation**, Armonk, NY (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 39 days.

(21) Appl. No.: **14/257,107**

(22) Filed: **Apr. 21, 2014**

(65) **Prior Publication Data**

US 2015/0304435 A1 Oct. 22, 2015

(51) **Int. Cl.**
H04L 29/08 (2006.01)
H04L 29/06 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 67/18*** (2013.01); ***H04L 63/08*** (2013.01); ***H04L 63/107*** (2013.01)

(58) **Field of Classification Search**
CPC H04L 63/107; H04L 63/108
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

7,747,645	B2	6/2010	Wahl	
2003/0065677	A1*	4/2003	Culp	G06Q 10/109
2004/0181602	A1*	9/2004	Fink	709/229
2008/0119958	A1*	5/2008	Bear	A61J 7/0481 700/244
2009/0113435	A1*	4/2009	Mizrachi	G06F 11/1461 718/102
2010/0175116	A1*	7/2010	Gum	726/6
2011/0202269	A1*	8/2011	Reventlow	701/201
2011/0246196	A1*	10/2011	Bhaskaran	G10L 17/24 704/235
2011/0296490	A1*	12/2011	Faitelson	G06F 21/6218 726/1
2013/0055370	A1	2/2013	Goldberg et al.	
2013/0109351	A1	5/2013	Kato	
2013/0218838	A1*	8/2013	Bevan	G06F 17/30129 707/626
2014/0012866	A1*	1/2014	Bowman	G06F 17/30634 707/755

OTHER PUBLICATIONS

Wikipedia, "Access control", From Wikipedia, the free encyclopedia, retrieved on Apr. 21, 2014 from website: <http://en.wikipedia.org/wiki/Access_control>.

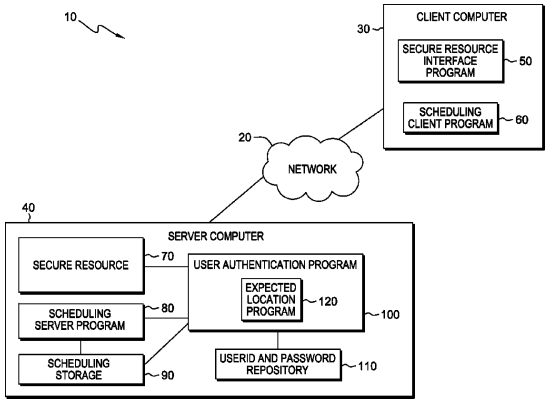
* cited by examiner

Primary Examiner — Samson Lemma
Assistant Examiner — Arya Golriz
(74) *Attorney, Agent, or Firm* — Edward J. Wixted, III

(57) **ABSTRACT**

In an approach for authenticating a user attempting to access to a resource, a processor receives an indication of a user attempting to access a resource within a timeframe, wherein the indication includes a location of the user. A processor identifies a location requirement for the user attempting to access the resource, wherein the location requirement originates from an entry indicating an expected location of the user within the timeframe, and wherein the entry is unmodifiable by the user. A processor determines whether the expected location of the user matches, within a threshold, the received location of the user attempting to access the resource.

16 Claims, 3 Drawing Sheets



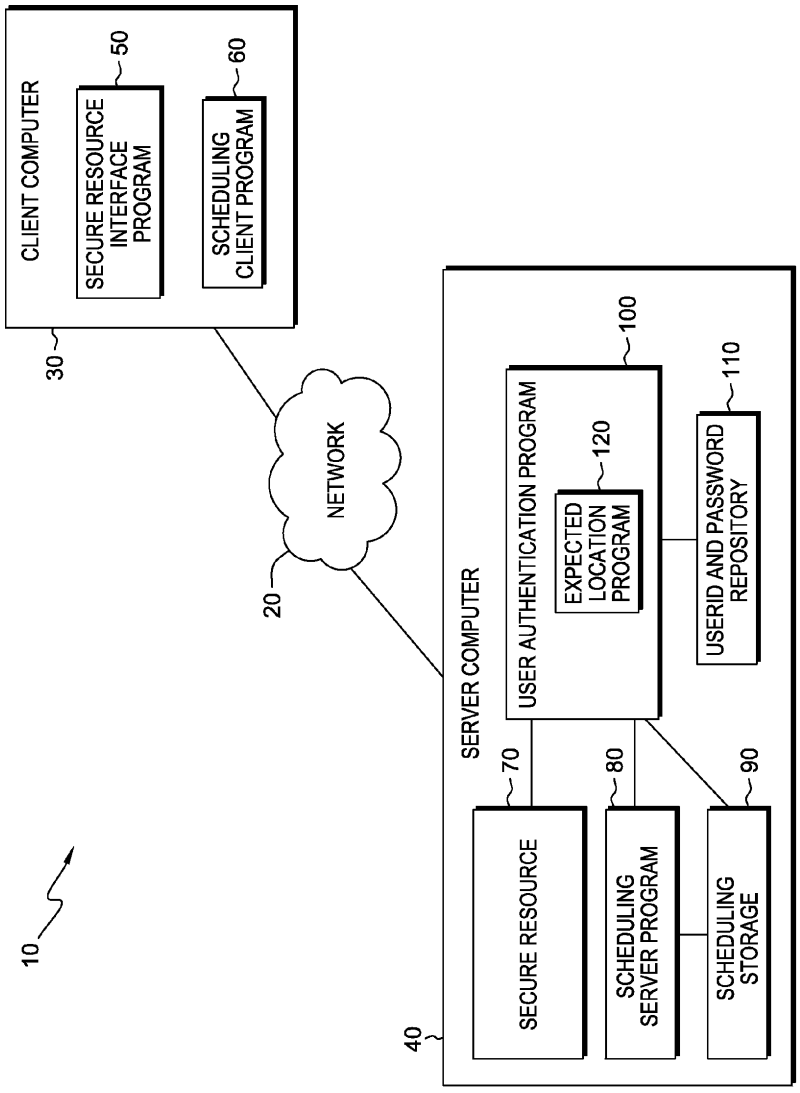

CLIENT COMPUTER
SECURE RESOURCE INTERFACE PROGRAM
50
SCHEDULING CLIENT PROGRAM
60
30
NETWORK
20
SERVER COMPUTER
USER AUTHENTICATION PROGRAM
100
EXPECTED LOCATION PROGRAM
120
USERID AND PASSWORD REPOSITORY
110
SECURE RESOURCE
70
SCHEDULING SERVER PROGRAM
80
SCHEDULING STORAGE
90
40
10

FIG. 1

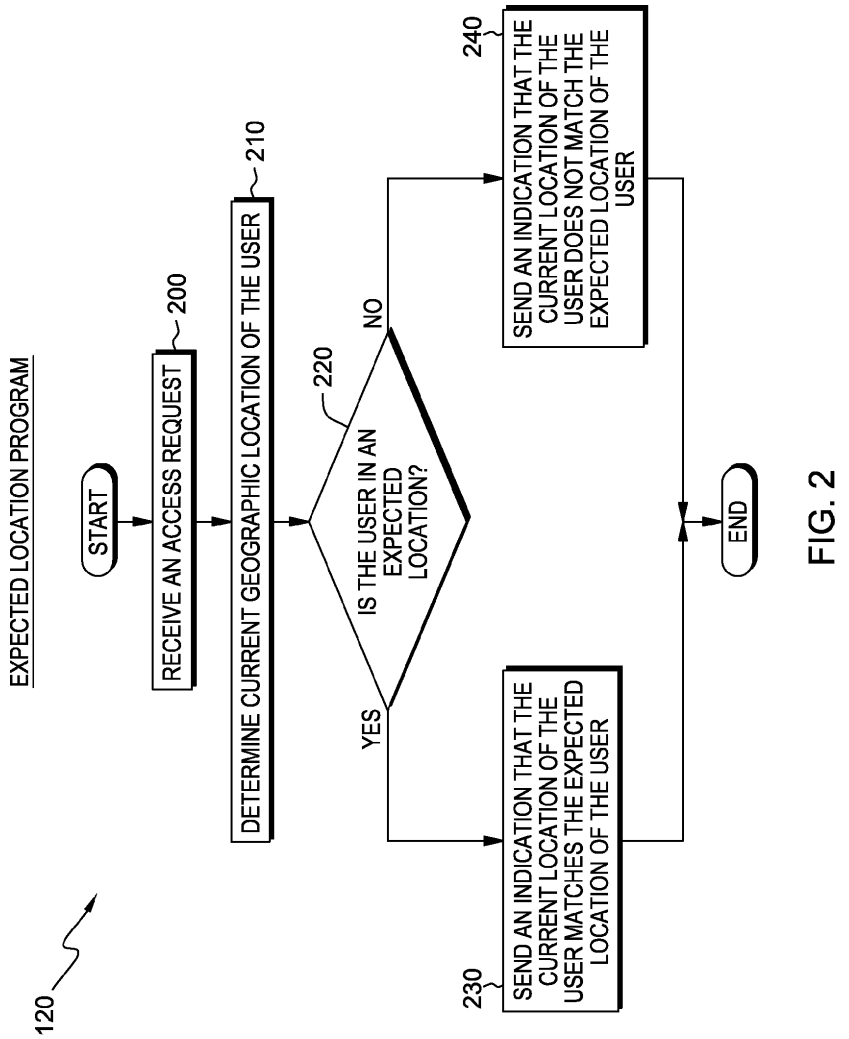

EXPECTED LOCATION PROGRAM
120
START
RECEIVE AN ACCESS REQUEST
200
DETERMINE CURRENT GEOGRAPHIC LOCATION OF THE USER
210
IS THE USER IN AN EXPECTED LOCATION?
220
YES
NO
SEND AN INDICATION THAT THE CURRENT LOCATION OF THE USER MATCHES THE EXPECTED LOCATION OF THE USER
230
SEND AN INDICATION THAT THE CURRENT LOCATION OF THE USER DOES NOT MATCH THE EXPECTED LOCATION OF THE USER
240
END

FIG. 2

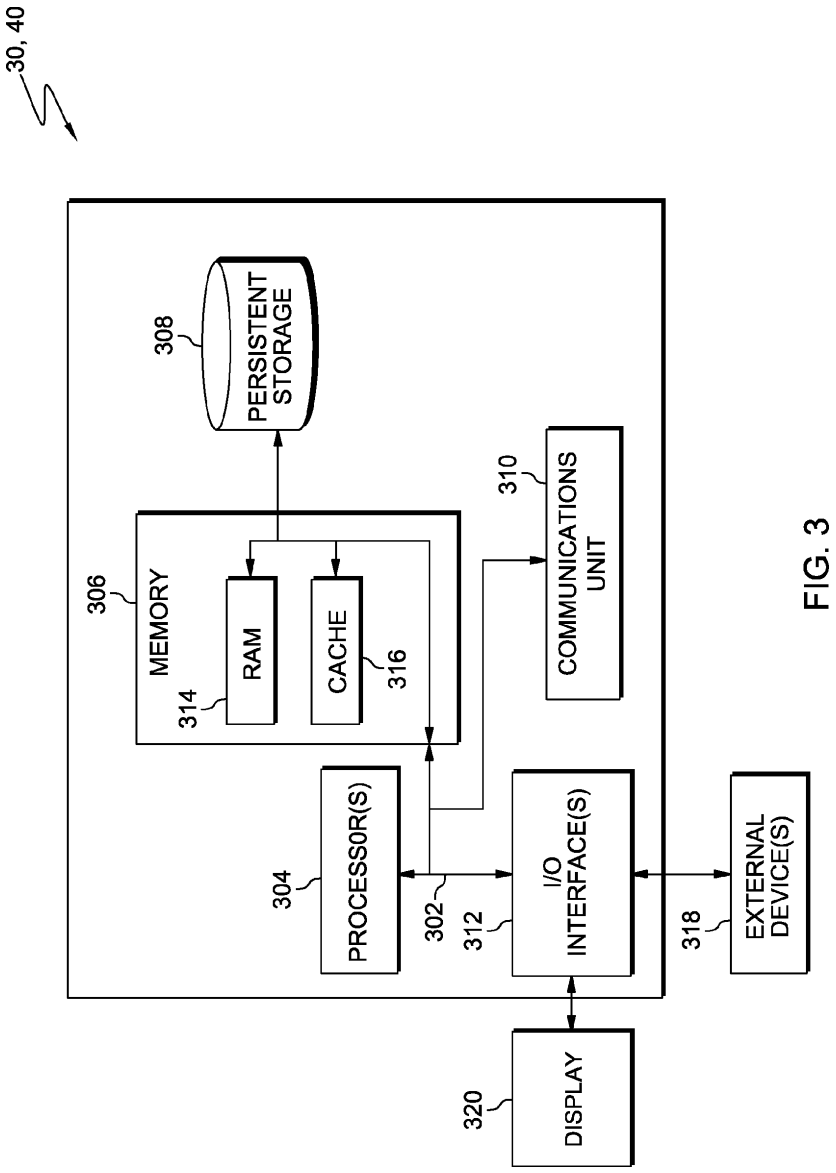

30, 40
308
PERSISTENT STORAGE
310
COMMUNICATIONS UNIT
306
MEMORY
RAM
314
CACHE
316
304
PROCESSOR(S)
302
312
I/O INTERFACE(S)
318
EXTERNAL DEVICE(S)
320
DISPLAY

FIG. 3

EXPECTED LOCATION-BASED ACCESS CONTROL

FIELD OF THE INVENTION

The present invention relates generally to access control, and more particularly to geographically-based access control.

BACKGROUND OF THE INVENTION

Computer networks, particularly those with global reach such as the Internet, have greatly influenced the way transactions are conducted and the way data is stored and retrieved. With the growth of the Internet, user authentication has become increasingly important for both computer systems and networks. Secure access to computer systems and computer networks has been traditionally implemented using a user identification (userid) and password pair. This requires the user to protect their userid and password from unauthorized use. If the userid and password are not protected, accounts and files can be compromised. For example, if a first user knows the userid and password of a second user, then the first user may easily access the second user's account information without being authorized to do so.

SUMMARY

Aspects of an embodiment of the present invention disclose a method, computer program product, and computing system for authenticating a user attempting to access to a resource. A processor receives an indication of a user attempting to access a resource within a timeframe, wherein the indication includes a location of the user. A processor identifies a location requirement for the user attempting to access the resource, wherein the location requirement originates from an entry indicating an expected location of the user within the timeframe, and wherein the entry is unmodifiable by the user. A processor determines whether the expected location of the user at least matches, within a threshold, the received location of the user attempting to access the resource.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

FIG. **1** is a functional block diagram illustrating a distributed data processing environment, in accordance with one embodiment of the present invention.

FIG. **2** is a flowchart depicting operational steps of an expected location program, executing within the environment of FIG. **1**, for determining whether a current location of a user matches an expected location of a user, in accordance with one embodiment of the present invention.

FIG. **3** depicts a block diagram of components of the server computer and the client computer of FIG. **1**, in accordance with one embodiment of the present invention.

DETAILED DESCRIPTION

The present invention will now be described in detail with reference to the Figures. FIG. **1** depicts a diagram of distributed data processing environment **10**, in accordance with one embodiment of the present invention. FIG. **1** provides only an illustration of one embodiment and does not imply any limitations with regard to the environments in which different embodiments may be implemented.

Distributed data processing environment **10** includes client computer **30** and server computer **40** interconnected over network **20**. Network **20** may be a local area network (LAN), a wide area network (WAN) such as the Internet, a combination of the two or any combination of connections and protocols that will support communications between client computer **30** and server computer **40**, in accordance with embodiments of the present invention. Network **20** may include wired, wireless, or fiber optic connections. Distributed data processing environment **10** may include additional server computers, client computers, or other devices not shown.

Client computer **30** may be a desktop computer, laptop computer, tablet computer, personal digital assistant (PDA), or smart phone. In general, client computer **30** may be any electronic device or computing system capable of processing computer program instructions, sending and receiving data, and communicating with server computer **40** over network **20**, in accordance with embodiments of the present invention. In the depicted embodiment, client computer **30** includes secure resource interface program **50** and scheduling client program **60**. In one embodiment, client computer **30** includes components described in reference to FIG. **3**.

Server computer **40** may be a management server, a web server, or any other electronic device or computing system capable of processing computer program instructions and receiving and sending data. In the depicted embodiment, server computer **40** may represent a server computing system utilizing multiple computers as a server system, such as in a cloud computing environment. In the depicted embodiment, server computer **40** includes secure resource **70**, scheduling server program **80**, scheduling storage **90**, user authentication program **100**, user identification (userid) and password repository **110**, and expected location program **120**. In one embodiment, server computer **40** includes components described in reference to FIG. **3**.

Secure resource **70** may be a website, a database, a data structure, or any computer resource or device that requires user authentication to access. In the depicted embodiment, secure resource **70** resides on server computer **40**. In other embodiments, secure resource **70** may reside on another server or another computing device, provided that secure resource **70** is accessible to secure resource interface program **50** and user authentication program **100**.

Secure resource interface program **50** operates to visualize content, such as menus and icons, and to allow a user to interact with applications or resources accessible to client computer **30**, such as secure resource **70** on server computer **40**, over network **20**. In one embodiment, secure resource interface program **50** may be a web browser. In other embodiments, secure resource interface program **50** may be an application on a smart phone, a security system program, or any other program or application capable of visualizing content and allowing a user to interact with applications or resources accessible to client computer **30**, such as secure resource **70** on server computer **40**, over network **20**.

Scheduling client program **60** may be a dedicated client scheduling program, a function integrated within another program, or any other program or function that can communicate with scheduling server program **80** over network **20** to provide a user interface for creating, receiving and responding to schedules and/or entries. In one embodiment, a schedule or entry may be a document that includes at least one scheduled activity. For example, a scheduled activity may be a meeting, appointment, travel plan, or any other event. A schedule or entry may include dates and times for scheduled activities. In addition, a schedule or entry may

include at least one geographic location at which each respective scheduled activity is intended to take place. A schedule or entry may also include regularly scheduled activities, such as a work schedule of a user. In some embodiments, when adding a scheduled activity to a schedule or entry, the user may include at least one geographic location indicating where the scheduled activity takes place. In some embodiments, schedules and entries may be managed by a third party, such as an employer, hotel, travel agency, or other entity. In some embodiments, the user may not have the ability to alter the schedule. For example, a user may not be able to change the entry indicating the user's work schedule. Such an entry may need to be changed by the user's employer. In one embodiment, scheduling client program **60** resides on client computer **30**. In other embodiments, scheduling client program **60** may reside on another server or another computing device, provided that scheduling server program **60** can communicate with scheduling server program **80**.

A user at client computer **30** may use scheduling client program **60** to add, remove, or modify a scheduled activity. In one embodiment, a user at client computer **30** uses scheduling client program **60** to modify his or her schedule. For example, the user may add an appointment to his or her schedule. In another example, a user may add regularly scheduled activities to his or her schedule, such as his or her work schedule. In yet another embodiment, scheduling client program **60** automatically receives the schedule of the user from another program (not shown). In yet another embodiment, scheduling client program **60** accesses a schedule stored by another program (not shown). In some embodiments, a user may have the ability to view his or her schedule, but the user may not have the ability to modify his or her schedule. In such an embodiment, a third party may be responsible for modifying the schedule. For example, an employer may establish and populate a work schedule and/or vacation schedule, and a travel agency may manage a travel itinerary. In such examples, the schedule/itinerary may be unmodifiable by the user.

In some embodiments, a user at client computer **30** may use scheduling client program **60** to modify a schedule of a second user. For example, the user may be a travel agent, and the travel agent may modify the schedule for a client. In such an example, the user may use scheduling client program **60** to modify the schedule of the second user to include travel plans of the second user. For example, the user adds a travel itinerary to the second user's schedule. In another example, the user enters a work schedule and associated location of a second user. In such an embodiment, the second user may not have the authority or privilege to independently adjust their schedule. A scheduling user may have an interest in securing secure resource **70**, and by controlling the schedule of a second user, the scheduling user may limit the locations from which the second user can access secure resource **70**. Scheduling client program **60** may periodically send updated schedules to scheduling server program **80** over network **20**. In another embodiment, scheduling client program **60** periodically sends schedules of users to expected location program **120** over network **20**. For example, scheduling client program **60** sends a modified schedule of a user to expected location program **120** over network **20**.

Scheduling server program **80** operates to receive, forward, and manage schedules received from scheduling client programs, such as scheduling client program **60**, located on client computer **30** and/or other client computers (not shown). In one embodiment, scheduling server program **80** stores scheduling events managed by scheduling server program **80** to scheduling storage **90**. In one embodiment, scheduling server program **80** periodically sends schedules of one or more users to expected location program **120**. For example, scheduling server program **80** may send a modified schedule of a user to expected location program **120**. In one embodiment, scheduling server program **80** resides on server computer **40**. In other embodiments, scheduling server program **80** may reside on another server or another computing device, provided that scheduling server program **80** can communicate with scheduling client program **60**, scheduling storage **90**, and expected location program **120**.

Scheduling storage **90** is a repository that may be written and read by scheduling server program **80** and may be accessible to scheduling server program **80**, user authentication program **100**, and expected location program **120**. In one embodiment, scheduling storage **90** stores schedules and/or entries associated with users of scheduling server program **80**. In some embodiments, scheduling storage **90** is a database. In other embodiments, scheduling storage **90** is a file. In some embodiment, scheduling storage **90** is located on server computer **40**. In other embodiments, scheduling storage **90** may be located on another server computer or another computing device, provided that scheduling storage **90** is accessible to scheduling server program **80**, user authentication program **100**, and expected location program **120**.

User authentication program **100** operates to determine whether to grant or deny a current user of client computer **30** access to secure resource **70** by determining if a userid and password, received from secure resource interface program **50**, matches a stored userid and password of a user authorized to access secure resource **70**. In one embodiment, user authentication program **110** accesses userid and password repository **110** and compares the userid and password sent by secure resource interface program **50** to the userids and corresponding passwords stored in userid and password repository **110**. In one embodiment, user authentication program **100** is a program residing on server computer **40**. In other embodiments, user authentication program **100** may reside on another server or another computing device, provided that user authentication program **100** is accessible to secure resource interface program **50** and secure resource **70** and has access to userid and password repository **110** and expected location program **120**.

Userid and password repository **110** is a repository that may be written to and read by user authentication program **110**. Userid and password repository **110** operates to store userids and corresponding passwords for users authorized to access secure resource **70**. In one embodiment, userid and password repository **110** is a database. In one embodiment, userid and password repository **110** is located on server computer **40**. In other embodiments, userid and password repository **110** may be located on another server computer or another computing device, provided that userid and password repository **110** is accessible to user authentication program **100**.

Expected location program **120** operates to determine whether a current location of a user matches an expected location of the user. In one embodiment, expected location program **120** receives an indication from user authentication program **100** that a user at client computer **30** is attempting to access secure resource **70**. In one embodiment, the indication includes the userid of the user. In some embodiments, the indication also includes the current geographic location of the user. In some embodiments, the indication is a geographic coordinate of the location of the user. In one embodiment, expected location program **120** is a function of

user authentication program **110**. In another embodiment, expected location program **120** is a stand-alone program. In one embodiment, expected location program **120** is located on server computer **40**. In other embodiments, expected location program **120** may be located on another server computer or another computing device, provided that expected location program **120** has access to secure resource **70**, scheduling storage **90**, and userid and password repository **110**.

In one embodiment, expected location program **120** accesses scheduling storage **90**. In such an embodiment, expected location program **120** may parse through schedules or entries stored by scheduling storage **90**. Expected location program **120** may identify a schedule or entry for the user associated with the received userid. Expected location program **120** may determine the geographic location where the user is scheduled to be based on the identified schedule or entry. For example, expected location program **120** determines from a schedule provided by a travel agency or employer that a user has travel plans and is scheduled to be in Spain during a specified timeframe. Expected location program **120** compares the user's current location (e.g. Madrid, Spain) to the users expected location (e.g. Spain). Expected location program **120** may determine that the user's current location matches the user's expected location. In some embodiments, expected location program **120** may determine that the user's current location matches the user's expected location within a predefined threshold. The predefined threshold may indicate a set of coordinates, location, or other location identifying means around the expected location within which, the user is considered to match, or partially match the expected location. Expected location program **120** may send an indication to user authentication program **100** indicating that the user's current location matches, or substantially matches, the user's expected location.

FIG. **2** depicts a flowchart of the steps of expected location program **120** for determining whether a current location of a user matches an expected location of a user, in accordance with one embodiment of the present invention.

Initially, in one embodiment, a user at client computer **30** uses secure resource interface program **50** to attempt to access secure resource **70** over network **20**. In some embodiments, the user enters a userid and password. Secure resource interface program **50** sends the userid and password for the user to user authentication program **100** over network **20**. In one embodiment, secure resource interface program **50** further includes information indicating the geographic location of the computing device associated with the user, such as client computer **30**. In one embodiment, secure resource interface program **50** sends an IP address of the user to user authentication program **100**. In other embodiments, secure resource interface program **50** may send GPS coordinates, RFID tag information, or utilize triangulation techniques to indicate the geographic location of client computer **30**.

User authentication program **100** receives the userid, password, and IP address (or other information used to locate the current geographic location of the user). In one embodiment, user authentication program **100** accesses userid and password repository **110** and compares the received password to the stored password for the received userid. User authentication program **100** determines that the received password matches the stored password for the userid. In one embodiment, user authentication program **100** sends an access request to expected location program **120**. In another embodiment, user authentication program **100** sends an access request to expected location program **120** before user authentication program **100** authenticates the userid and password of the user.

In step **200**, expected location program **120** receives an access request. In one embodiment, expected location program **120** receives an access request from user authentication program **100**. The access request can include the userid and a geographic location of the user at client computer **30**.

In step **210**, expected location program **120** determines a current geographic location of the user. In one embodiment, expected location program **120** uses the received IP address to determine the current geographic location of the user. Expected location program **120** may determine the geographic location of client computer **30** and the user based on a received IP address. An IP address is a numerical label assigned to a device (e.g. client computer **30** or server computer **40**) in a computer network (e.g. network **20**) that uses the Internet Protocol for communication. An IP address serves two principal functions: 1) network interface identification, and 2) geographic location addressing. In one example, expected location program **120** determines, from the received IP address, that the current geographic location of the user is Los Angeles, Calif.

In other embodiments, expected location program **120** determines the location using global positioning system (GPS) coordinates received from client computer **30**, when client computer **30** is a computing device with GPS capabilities, such as a smartphone or tablet. In another embodiment, client computer **30** may not have GPS capabilities, and expected location program **120** receives GPS coordinates of the user from an external device in the user's possession, such as a GPS receiver, cell phone, tablet, or other external device capable of communicating with client computer **30**. In yet another embodiment, when client computer **30** is connected to a cellular network, expected location program **120** may receive the geographic location of a user gathered via the multilateration of radio signals between radio towers of the network and client computer **30**. In yet another embodiment, expected location program **120** receives information and determines the geographic location of a user from a badging or check-in system. For example, an RFID system may be implemented within an office building that can communicate with server **30** based on active or passive RFID tags located on a user's badge, client device, or any other object or device compatible with an RFID tag. Multiple RFID tag readers may be positioned throughout the office building so that the location of the user can be determined. In other embodiments, expected location program **120** determines the current geographic location of the user from connections to specific networks. In other embodiments expected location program **120** determines the current geographic location of the user from telephone numbers or connections to specific networks.

In decision **220**, expected location program **120** determines if client computer **30**, and therefore the user, is at an expected location. The expected location may be a location requirement for the user to access secure resource **70**. In some embodiments, the expected location originates from a schedule or entry. In one embodiment, expected location program **120** accesses scheduling storage **90** and identifies a schedule, travel itinerary, calendar, or other document specifying dates and locations where the user is expected, associated with the userid received from client computer **30**. In some embodiments, the schedule or other entry was created, modified, and/or maintained by the user. In other embodiments, the schedule or other entry was created, modified, and/or maintained by a third party, such as an employer,

travel agency, or other entity, and the user does not have access to adjust or otherwise modify the schedule or entry. In such an embodiment, the third party may have an interest in limiting access to secure resource **70**. For example, an employer may want to make sure an employee, with legitimate purpose, is accessing secure resource **70** during actual business hours or at particular business locations. In addition, denying a user the ability to modify the schedule or entry may prevent fraudulent access by another individual attempting to modify the schedule to their present location in order to gain access to secure resource **70**.

In one embodiment, expected location program **120** uses text analytics to parse through the schedule or other document. Using natural language processing and at least one set of dictionaries and rules, expected location program **120** can perform text analytics on the schedule or other document. Text analytics can be performed using an Unstructured Information Management Architecture (UIMA) application configured to analyze unstructured information to discover patterns relevant to expected location program **120** by processing plain text and identifying entities or relations.

In another embodiment, expected location program **120** accesses an e-mail repository to identify e-mail correspondence associated with the received userid. Expected location program **120** may use text analytics to parse through the e-mail correspondence. In one embodiment, expected location program **120** uses natural language processing and at least one set of dictionaries and rules to determine the user's expected location from the user's e-mail correspondence. For example, expected location program **120** determines from the e-mail correspondence that the user has travel plans to visit a friend in Los Angeles, Calif. on the current date.

In yet another embodiment, expected location program **120** accesses a cell phone memory repository, such as a memory card associated with the received userid. Expected location program **120** uses text analytics to parse through a text message correspondence. In one embodiment, expected location program **120** uses natural language processing and at least one set of dictionaries and rules to determine the user's expected location from the user's text message correspondence. For example, expected location program **120** determines from the text message correspondence that the user has travel plans to visit a friend in Los Angeles, Calif. on the current date.

In another embodiment, expected location program **120** receives the expected location of the user from scheduling server program **80**. In another embodiment, expected location program **120** receives the expected location of the user from scheduling client program **60**. In yet another embodiment, expected location program **120** accesses information stored by a scheduling program, such as scheduling server program **80** to scheduling storage **90**, and retrieves a list of expected locations and corresponding dates and/or times within which the user is anticipated to be at the expected location. In such an embodiment, scheduling server program **80** may analyze entry information to determine a location and date or time associated with the entry using text analytic techniques previously described and/or information located in fields of the entry associated with location and date and/or time.

Expected location program **120** compares the user's current location (determined in step **210**) to the one or more expected locations of the user. In decision **220**, expected location program **120** determines if the user's current location matches the user's expected location. In one embodiment, expected location program **120** determines if the user's current location exactly matches the user's expected location. In another embodiment, expected location program **120** determines if the user's current location is within a pre-defined threshold, such as a radius, of the user's expected location. For example, expected location program **120** determines if the user's current location is within a 50 mile radius of the user's expected location. Alternatively, expected location program **120** may determine if the user's current location is within a certain set of GPS coordinates that define a boundary of a specified distance around the expected location. In another embodiment, expected location program **120** may determine if the IP address associated with the user matches an IP address corresponding to an expected location, such as a town or city. If expected location program **120** determines that the user's current location matches the user's expected location, expected location program **120** proceeds to step **230** (decision **220**, yes branch). If expected location program **120** determines that the user's current location does not match the user's expected location, expected location program **120** proceeds to step **240** (decision **220**, no branch).

In step **230**, expected location program **120** sends an indication that the current location of the user matches the expected location of the user. In one embodiment, expected location program **120** sends an indication that the current location of the user matches the expected location of the user to user authentication program **100**. In one embodiment, user authentication program **100** allows the user to access secure resource **70**. In another embodiment, user authentication program **100** compares the received userid and password to the userid(s) and password(s) stored by userid and password repository **110**. In yet another embodiment, expected location program **120** allows the user to access secure resource **70**.

In step **240**, expected location program **120** sends an indication that the current location of the user does not match the expected location of the user. In one embodiment, expected location program **120** sends an indication that the current location of the user does not match the expected location of the user to user authentication program **100**. In one embodiment, user authentication program **100** does not allow the user to access secure resource **70**. In another embodiment, expected location program **120** does not allow the user to access secure resource **70**. In yet another embodiment, expected location program **120** alerts the host or administrator of secure resource **70** that the user has attempted to access secure resource **70** from an unexpected location. In yet another embodiment, expected location program **120** requires the user to provide additional authentication. For example, expected location program **120** may prompt the user to enter personal information, such as the date of birth of the user. In another embodiment, expected location program **120** prompts the user to enter a second password. In yet another embodiment, expected location program **120** requires the user to provide biometric authentication. For example, expected location program **120** prompts the user to speak into a microphone. In such an embodiment, expected location program **120** compares the user's voice to a stored voice associated with the userid and password combination entered by the user. In another embodiment, expected location program **120** requires a security token, or software token, as additional authentication. A software token is a type of two-factor authentication security device that may be used to authorize the use of computer services. Software tokens can be stored on a general-purpose electronic device such as a desktop computer, laptop, PDA, or mobile phone and can be duplicated.

FIG. **3** depicts a block diagram of components of client computer **30** and server computer **40** in accordance with one embodiment of the present invention. It should be appreciated that FIG. **3** provides only an illustration of one implementation and does not imply any limitations with regard to the environments in which different embodiments may be implemented. Many modifications to the depicted environment may be made.

Client computer **30** and server computer **40** can each include communications fabric **302**, which provides communications between computer processor(s) **304**, memory **306**, persistent storage **308**, communications unit **310**, and input/output (I/O) interface(s) **312**. Communications fabric **302** can be implemented with any architecture designed for passing data and/or control information between processors (such as microprocessors, communications and network processors, etc.), system memory, peripheral devices, and any other hardware components within a system. For example, communications fabric **302** can be implemented with one or more buses.

Memory **306** and persistent storage **308** are computer-readable storage media. In this embodiment, memory **306** includes random access memory (RAM) **314** and cache memory **316**. In general, memory **306** can include any suitable volatile or non-volatile computer-readable storage media.

Secure resource interface program **50** and scheduling client program **60** is stored in persistent storage **308** of client computer **30** for execution by one or more of the respective computer processors **304** of client computer **30** via one or more memories of memory **306** of client computer **30**. Secure resource **70**, scheduling server program **80**, scheduling storage **90**, user authentication program **100**, userid and password repository **110**, and expected location program **120** are stored in persistent storage **308** of server computer **40** for execution and/or access by one or more of the respective computer processors **304** of server computer **40** via one or more memories of memory **306** of server computer **40**. In this embodiment, persistent storage **308** includes a magnetic hard disk drive. Alternatively, or in addition to a magnetic hard disk drive, persistent storage **308** can include a solid state hard drive, a semiconductor storage device, read-only memory (ROM), erasable programmable read-only memory (EPROM), flash memory, or any other computer-readable storage media capable of storing program instructions or digital information.

The media used by persistent storage **308** may also be removable. For example, a removable hard drive may be used for persistent storage **308**. Other examples include optical and magnetic disks, thumb drives, and smart cards inserted into a drive for transfer onto another computer-readable storage medium that is also part of persistent storage **308**.

Communications unit **310**, in these examples, provides for communications with other servers or devices. In these examples, communications unit **310** includes one or more network interface cards. Communications unit **310** may provide communications through the use of either or both physical and wireless communications links. Secure resource interface program **50** and scheduling client program **60** may be downloaded to persistent storage **308** of client computer **30** through the communications unit **310** of client computer **30**. Secure resource **70**, scheduling server program **80**, scheduling storage **90**, user authentication program **100**, userid and password repository **110**, and expected location program **120** may be downloaded to persistent storage **308** of server computer **40** through the communications unit **310** of server computer **40**.

I/O interface(s) **312** allows for input and output of data with other devices that may be connected to client computer **30** or server computer **40**. For example, I/O interface **312** may provide a connection to external devices **318** such as a keyboard, keypad, a touch screen, and/or some other suitable input device. External devices **318** can also include portable computer-readable storage media such as, for example, thumb drives, portable optical or magnetic disks, and memory cards. Software and data used to practice embodiments of the present invention, e.g., secure resource interface program **50** and scheduling client program **60**, can be stored on such portable computer-readable storage media and can be loaded onto persistent storage **308** of client computer **30**, respectively, via the respective I/O interface(s) **312** of client computer **30**. Software and data used to practice embodiments of the present invention, e.g. Secure resource **70**, scheduling server program **80**, scheduling storage **90**, user authentication program **100**, userid and password repository **110**, and expected location program **120**, can be stored on such portable computer-readable storage media and can be loaded onto persistent storage **308** of server computer **40** via I/O interface(s) **312** of server computer **40**.

The programs described herein are identified based upon the application for which they are implemented in a specific embodiment of the invention. However, it should be appreciated that any particular program nomenclature herein is used merely for convenience, and thus the invention should not be limited to use solely in any specific application identified and/or implied by such nomenclature.

The present invention may be a system, a method, and/or a computer program product. The computer program product may include a computer readable storage medium (or media) having computer readable program instructions thereon for causing a processor to carry out aspects of the present invention.

The computer readable storage medium can be a tangible device that can retain and store instructions for use by an instruction execution device. The computer readable storage medium may be, for example, but is not limited to, an electronic storage device, a magnetic storage device, an optical storage device, an electromagnetic storage device, a semiconductor storage device, or any suitable combination of the foregoing. A non-exhaustive list of more specific examples of the computer readable storage medium includes the following: a portable computer diskette, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or Flash memory), a static random access memory (SRAM), a portable compact disc read-only memory (CD-ROM), a digital versatile disk (DVD), a memory stick, a floppy disk, a mechanically encoded device such as punch-cards or raised structures in a groove having instructions recorded thereon, and any suitable combination of the foregoing. A computer readable storage medium, as used herein, is not to be construed as being transitory signals per se, such as radio waves or other freely propagating electromagnetic waves, electromagnetic waves propagating through a waveguide or other transmission media (e.g., light pulses passing through a fiber-optic cable), or electrical signals transmitted through a wire.

Computer readable program instructions described herein can be downloaded to respective computing/processing devices from a computer readable storage medium or to an external computer or external storage device via a network,

for example, the Internet, a local area network, a wide area network and/or a wireless network. The network may comprise copper transmission cables, optical transmission fibers, wireless transmission, routers, firewalls, switches, gateway computers and/or edge servers. A network adapter card or network interface in each computing/processing device receives computer readable program instructions from the network and forwards the computer readable program instructions for storage in a computer readable storage medium within the respective computing/processing device.

Computer readable program instructions for carrying out operations of the present invention may be assembler instructions, instruction-set-architecture (ISA) instructions, machine instructions, machine dependent instructions, microcode, firmware instructions, state-setting data, or either source code or object code written in any combination of one or more programming languages, including an object oriented programming language such as Smalltalk, C++ or the like, and conventional procedural programming languages, such as the "C" programming language or similar programming languages. The computer readable program instructions may execute entirely on the user's computer, partly on the user's computer, as a stand-alone software package, partly on the user's computer and partly on a remote computer or entirely on the remote computer or server. In the latter scenario, the remote computer may be connected to the user's computer through any type of network, including a local area network (LAN) or a wide area network (WAN), or the connection may be made to an external computer (for example, through the Internet using an Internet Service Provider). In some embodiments, electronic circuitry including, for example, programmable logic circuitry, field-programmable gate arrays (FPGA), or programmable logic arrays (PLA) may execute the computer readable program instructions by utilizing state information of the computer readable program instructions to personalize the electronic circuitry, in order to perform aspects of the present invention.

Aspects of the present invention are described herein with reference to flowchart illustrations and/or block diagrams of methods, apparatus (systems), and computer program products according to embodiments of the invention. It will be understood that each block of the flowchart illustrations and/or block diagrams, and combinations of blocks in the flowchart illustrations and/or block diagrams, can be implemented by computer readable program instructions.

These computer readable program instructions may be provided to a processor of a general purpose computer, special purpose computer, or other programmable data processing apparatus to produce a machine, such that the instructions, which execute via the processor of the computer or other programmable data processing apparatus, create means for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks. These computer readable program instructions may also be stored in a computer readable storage medium that can direct a computer, a programmable data processing apparatus, and/or other devices to function in a particular manner, such that the computer readable storage medium having instructions stored therein comprises an article of manufacture including instructions which implement aspects of the function/act specified in the flowchart and/or block diagram block or blocks.

The computer readable program instructions may also be loaded onto a computer, other programmable data processing apparatus, or other device to cause a series of operational steps to be performed on the computer, other programmable apparatus or other device to produce a computer implemented process, such that the instructions which execute on the computer, other programmable apparatus, or other device implement the functions/acts specified in the flowchart and/or block diagram block or blocks.

The flowchart and block diagrams in the Figures illustrate the architecture, functionality, and operation of possible implementations of systems, methods, and computer program products according to various embodiments of the present invention. In this regard, each block in the flowchart or block diagrams may represent a module, segment, or portion of instructions, which comprises one or more executable instructions for implementing the specified logical function(s). In some alternative implementations, the functions noted in the block may occur out of the order noted in the figures. For example, two blocks shown in succession may, in fact, be executed substantially concurrently, or the blocks may sometimes be executed in the reverse order, depending upon the functionality involved. It will also be noted that each block of the block diagrams and/or flowchart illustration, and combinations of blocks in the block diagrams and/or flowchart illustration, can be implemented by special purpose hardware-based systems that perform the specified functions or acts or carry out combinations of special purpose hardware and computer instructions.

What is claimed is:

1. A method for authenticating a user attempting to access to a resource, the method comprising:

receiving a schedule indicating an expected location of a user within a timeframe, wherein:

text contained in the schedule was populated by an entity and the schedule is unmodifiable by the user; and

the schedule is associated with a user identification unique to the user;

connecting a computing device of the user to a network;

receiving, from the computing device connected to the network, an indication, via the network, of the user attempting to access an electronic resource at a storage location that is accessible via the network, within the timeframe, wherein the indication includes the user identification unique to the user and a password;

determining, by one or more hardware processors, a location of the first user utilizing a radio-frequency identification (RFID) system and receiving RFID tag information associated with the user, wherein the RFID tag information was obtained from an RFID tag reader of the RFID system;

determining that the entity has authorized the user to access the electronic resource based on the user identification unique to the user and the password;

extracting an expected location of the user within the timeframe from unstructured text of the schedule using text analytics on the unstructured text of the schedule;

subsequent to determining that the user is a user authorized to access the electronic resource, determining whether the expected location of the user matches, within a threshold, the received location of the user attempting to access the electronic resource; and

performing an action based on the determination.

2. The method of claim **1**, wherein, responsive to determining that the expected location of the user matches, within the threshold, the received location of the user attempting to access the electronic resource, the action comprises causing the user to be granted access to the electronic resource.

3. The method of claim **1**, wherein, responsive to determining that the expected location of the user does not match,

within the threshold, the received location of the user attempting to access the electronic resource, the action comprises causing the user to be denied access to the electronic resource.

4. The method of claim **1**, wherein, responsive to determining that the expected location of the user does not match, within the threshold, the received location of the user attempting to access the electronic resource, the action comprises causing a biometric authentication requirement to be presented to the user, wherein the biometric authentication requirement includes, at least, a prompt for the user to speak into a microphone to compare the user's voice to a stored voice associated with the user identification.

5. The method of claim **1**, wherein, responsive to determining that the expected location of the user does not match, within the threshold, the received location of the user attempting to access the electronic resource, causing an alert to be provided to a host of the electronic resource.

6. A computer program product for securing access to a resource, the computer program product comprising:

one or more computer readable hardware storage devices and program instructions stored on the one or more computer readable hardware storage devices, the program instructions comprising:

program instructions to receive a schedule indicating an expected location of a user within a timeframe, wherein:

text contained in the schedule was populated by an entity and the schedule is unmodifiable by the user; and

the schedule is associated with a user identification unique to the user;

program instructions to connect a computing device of the user to a network;

program instructions to receive, from the computing device connected to the network, an indication, via the network, of the user attempting to access an electronic resource at a storage location that is accessible via the network, within the timeframe, wherein the indication includes the user identification unique to the user and a password;

program instructions to determine a location of the first user utilizing a radio-frequency identification (RFID) system and receiving RFID tag information associated with the user, wherein the RFID tag information was obtained from an RFID tag reader of the RFID system;

program instructions to determine that the entity has authorized the user to access the electronic resource based on the user identification unique to the user and the password;

program instructions to extract an expected location of the user within the timeframe from unstructured text of the schedule using text analytics on the unstructured text of the schedule;

program instructions to, subsequent to determining that the user is a user authorized to access the electronic resource, determine whether the expected location of the user matches, within a threshold, the received location of the user attempting to access the electronic resource; and

program instructions to perform an action based on the determination.

7. The computer program product of claim **6**, wherein, responsive to determining that the expected location of the user matches, within the threshold, the received location of the user attempting to access the electronic resource, the action comprises causing the user to be granted access to the electronic resource.

8. The computer program product of claim **6**, wherein, responsive to determining that the expected location of the user does not match, within the threshold, the received location of the user attempting to access the electronic resource, the action comprises causing the user to be denied access to the electronic resource.

9. The computer program product of claim **6**, wherein, responsive to determining that the expected location of the user does not match, within the threshold, the received location of the user attempting to access the electronic resource, the action comprises causing a biometric authentication requirement to be presented to the user, wherein the biometric authentication requirement includes, at least, a prompt for the user to speak into a microphone to compare the user's voice to a stored voice associated with the user identification.

10. The computer program product of claim **6**, wherein, responsive to determining that the expected location of the user does not match, within the threshold, the received location of the user attempting to access the electronic resource, the action comprises causing an alert to be provided to a host of the electronic resource.

11. A computer system for securing access to a resource, the computer system comprising:

one or more computer processors, one or more computer readable storage devices, and program instructions stored on the computer readable storage devices for execution by at least one of the one or more computer processors, the program instructions comprising:

program instructions to receive a schedule indicating an expected location of a user within a timeframe, wherein:

text contained in the schedule was populated by an entity and the schedule is unmodifiable by the user; and

the schedule is associated with a user identification unique to the user;

program instructions to connect a computing device of the user to a network;

program instructions to receive, from the computing device connected to the network, an indication, via the network, of the user attempting to access an electronic resource at a storage location that is accessible via the network within the timeframe, wherein the indication includes the user identification unique to the user and a password;

program instructions to determine a location of the first user utilizing a radio-frequency identification (RFID) system and receiving RFID tag information associated with the user, wherein the RFID tag information was obtained from an RFID tag reader of the RFID system;

program instructions to determine that the entity has authorized the user to access the electronic resource based on the user identification unique to the user and the password;

program instructions to extract an expected location of the user within the timeframe from unstructured text of the schedule using text analytics on the unstructured text of the schedule, wherein program instructions to extract the expected location of the user within the timeframe from the unstructured text of the schedule using text analytics on the unstructured text of the schedule comprise:

program instructions to parse the unstructured text of the schedule to identify at least the expected location of the user within the timeframe;

program instructions to, subsequent to determining that the user is a user authorized to access the electronic resource, determine whether the expected location of the user matches, within a threshold, the received location of the user attempting to access the resource; and

responsive to determining that the expected location of the user does not match, within the threshold, the received location of the user attempting to access the resource:

causing an alert to be provided to a host of the resource; and

causing a biometric authentication requirement to be presented to the user, wherein the biometric authentication requirement includes, at least, a prompt for the user to speak into a microphone to compare the user's voice to a stored voice associated with the user identification.

12. The computer system of claim **11**, wherein, responsive to determining that the expected location of the user matches, within the threshold, the received location of the user attempting to access the resource, the action comprises causing the user to be granted access to the resource.

13. The computer system of claim **11**, wherein, responsive to determining that the expected location of the user does not match, within the threshold, the received location of the user attempting to access the resource, the action comprises causing the user to be denied access to the resource.

14. The method of claim **1**, wherein the resource is a database.

15. The method of claim **1**, wherein the resource is a website.

16. The method of claim **1**, wherein extracting the expected location of the user within the timeframe from the unstructured text of the schedule using text analytics on the unstructured text of the schedule comprises:

parsing the unstructured text of the schedule to identify at least the expected location of the user within the timeframe.

* * * * *


US008838988B2

(12) **United States Patent**
Bravo et al.

(10) **Patent No.: US 8,838,988 B2**
(45) **Date of Patent: Sep. 16, 2014**

(54) **VERIFICATION OF TRANSACTIONAL INTEGRITY**

(75) Inventors: **Jose F. Bravo**, Mamaroneck, NY (US); **Jeffery L. Crume**, Raleigh, NC (US)

(73) Assignee: **International Business Machines Corporation**, Armonk, NY (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 1 day.

(21) Appl. No.: **13/084,823**

(22) Filed: **Apr. 12, 2011**

(65) **Prior Publication Data**

US 2012/0264405 A1 Oct. 18, 2012

(51) **Int. Cl.**
H04L 29/06 (2006.01)

(52) **U.S. Cl.**
USPC **713/183**

(58) **Field of Classification Search**
USPC 713/183
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,310,720	A	1/1982	Check, Jr.
5,046,082	A	9/1991	Zicker et al.
5,068,894	A	11/1991	Hoppe
5,323,465	A	6/1994	Avarne
5,457,737	A	10/1995	Wen
5,491,752	A	2/1996	Kaufman et al.
5,497,411	A	3/1996	Pellerin
5,657,388	A	8/1997	Weiss
5,684,950	A	11/1997	Dare et al.
5,701,339	A	12/1997	Suda
5,749,052	A	5/1998	Hidem et al.
5,841,871	A	11/1998	Pinkas
5,842,124	A	11/1998	Kenagy et al.
5,892,902	A	4/1999	Clark
5,953,422	A	9/1999	Angelo et al.
5,971,272	A	10/1999	Hsiao
6,000,031	A	12/1999	Bingaman et al.
6,169,890	B1	1/2001	Vatanen
6,278,863	B1	8/2001	Mabrouki

(Continued)

FOREIGN PATENT DOCUMENTS

EP	1119147	A1	7/2001
GB	2456509	A	7/2009

(Continued)

OTHER PUBLICATIONS

Transaction Verification, PhoneFactor Product Information, PhoneFactor Inc., Dec. 7, 2010, 1 page, http://www.webcitation.org/5unLaf84Y.

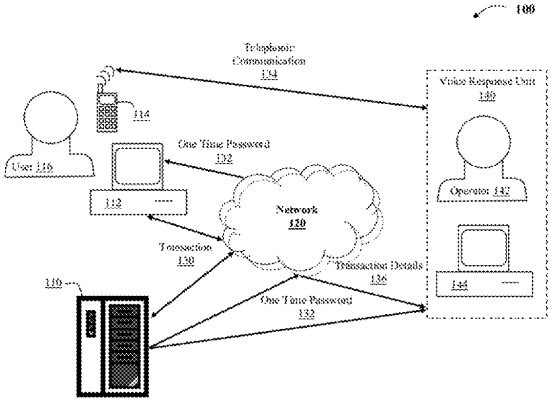
(Continued)

Primary Examiner — Jason Gee
(74) *Attorney, Agent, or Firm* — Doulgas A. Lashmit; Hoffman Warnick LLC

(57) **ABSTRACT**

Aspects of the present invention provide a solution for verifying the integrity of a transaction. In response to receipt of a confirmed electronic transaction from a user, a one time password is forwarded to the user. The user then initiates a telephonic communication with a verifier on the user's wireless device and provides the one time password to the verifier. The verifier authenticates the mobile telephonic device based on the device's caller identification number and determines whether the one time password provided by the user matches the one forwarded to the user. After the user is authenticated, the verifier communicates the details of the transaction that were received and the user confirms whether the details match those originally entered.

20 Claims, 2 Drawing Sheets



(56) **References Cited**

U.S. PATENT DOCUMENTS

6,308,268	B1	10/2001	Audebert	
6,324,271	B1	11/2001	Sawyer et al.	
6,330,608	B1	12/2001	Stiles	
6,334,056	B1	12/2001	Holmes et al.	
6,338,140	B1	1/2002	Owens et al.	
6,349,134	B1	2/2002	Katz	
6,385,729	B1	5/2002	DiGiorgio et al.	
6,387,729	B2	5/2002	Eng et al.	
6,393,468	B1	5/2002	McGee	
6,400,726	B1	6/2002	Piret et al.	
6,466,780	B1	10/2002	Geiselman et al.	
6,535,726	B1	3/2003	Johnson	
6,584,309	B1	6/2003	Whigham	
6,687,241	B1	2/2004	Goss	
6,707,915	B1	3/2004	Jobst et al.	
6,731,731	B1	5/2004	Ueshima	
6,993,658	B1	1/2006	Engberg et al.	
6,993,663	B1	1/2006	Paya et al.	
7,007,301	B2	2/2006	Crosbie et al.	
7,024,688	B1	4/2006	Faccin et al.	
7,028,179	B2	4/2006	Anderson et al.	
7,058,968	B2	6/2006	Rowland et al.	
7,100,204	B1	8/2006	Myllymaki et al.	
7,133,662	B2	11/2006	Bravo et al.	
7,142,840	B1	11/2006	Geddes et al.	
7,290,278	B2	10/2007	Cahill et al.	
7,337,431	B1	2/2008	Barnes et al.	
7,357,310	B2	4/2008	Calabrese et al.	
7,379,921	B1	5/2008	Kiliccote	
7,380,708	B1	6/2008	Kiliccote	
7,447,494	B2	11/2008	Law et al.	
7,519,989	B2	4/2009	Lin et al.	
7,540,022	B2	5/2009	Barrari et al.	
7,600,676	B1 *	10/2009	Rados et al.	235/380
7,665,128	B2	2/2010	Yang	
7,715,823	B2	5/2010	Bravo et al.	
7,716,742	B1	5/2010	Roesch et al.	
7,765,584	B2	7/2010	Roskind	
7,823,199	B1	10/2010	Rathi et al.	
7,845,004	B2	11/2010	Bardsley et al.	
7,886,346	B2	2/2011	Sandhu et al.	
7,926,108	B2	4/2011	Rand et al.	
7,930,540	B2	4/2011	Ahuja et al.	
7,954,150	B2	5/2011	Croft et al.	
8,151,327	B2	4/2012	Eisen	
8,181,248	B2	5/2012	Oh et al.	
8,285,639	B2	10/2012	Eden et al.	
8,302,180	B1	10/2012	Gudov et al.	
2001/0054155	A1	12/2001	Hagan et al.	
2002/0069165	A1	6/2002	O'Neil	
2002/0091931	A1	7/2002	Quick et al.	
2002/0095588	A1	7/2002	Shigematsu et al.	
2002/0178070	A1	11/2002	Leveridge	
2002/0178370	A1	11/2002	Gurevich et al.	
2003/0014315	A1	1/2003	Jaalinoja et al.	
2003/0154382	A1	8/2003	Vicard	
2003/0172272	A1	9/2003	Ehlers et al.	
2004/0148520	A1	7/2004	Talpade et al.	
2004/0152446	A1	8/2004	Saunders et al.	
2004/0198329	A1	10/2004	Vasa	
2004/0243856	A1 *	12/2004	Shatford	713/202
2005/0015624	A1	1/2005	Ginter et al.	
2005/0022020	A1	1/2005	Fremberg	
2005/0182958	A1	8/2005	Pham et al.	
2005/0188423	A1	8/2005	Motsinger et al.	
2005/0210251	A1	9/2005	Nyberg et al.	
2006/0094403	A1	5/2006	Norefors et al.	
2006/0095955	A1	5/2006	Vong et al.	
2006/0179304	A1 *	8/2006	Han	713/168
2006/0248021	A1	11/2006	Jain et al.	
2006/0288411	A1	12/2006	Garg et al.	
2007/0015492	A1 *	1/2007	Bravo et al.	455/411
2007/0067828	A1	3/2007	Bychkov	
2007/0084913	A1	4/2007	Weston	
2007/0107050	A1	5/2007	Selvarajan	
2007/0136573	A1	6/2007	Steinberg	
2007/0136808	A1	6/2007	Xiong	
2007/0143851	A1	6/2007	Nicodemus et al.	
2007/0186099	A1	8/2007	Beck et al.	
2007/0220275	A1 *	9/2007	Heitzeberg et al.	713/186
2007/0234426	A1	10/2007	Khanolkar et al.	
2007/0261112	A1	11/2007	Todd et al.	
2007/0266257	A1	11/2007	Camaisa et al.	
2008/0028447	A1	1/2008	O'Malley et al.	
2008/0172730	A1	7/2008	Sandhu et al.	
2008/0181380	A1	7/2008	Gustave et al.	
2008/0189776	A1	8/2008	Constable	
2008/0209275	A1	8/2008	Kwan et al.	
2008/0270301	A1	10/2008	Jones et al.	
2008/0281737	A1	11/2008	Fajardo	
2008/0318548	A1	12/2008	Bravo et al.	
2009/0037329	A1	2/2009	Coppinger et al.	
2009/0077637	A1	3/2009	Santos et al.	
2009/0094682	A1	4/2009	Sage et al.	
2009/0095588	A1	4/2009	Thomas	
2009/0104889	A1	4/2009	Lotvonen et al.	
2009/0106138	A1	4/2009	Smith et al.	
2009/0300738	A1	12/2009	Dewe et al.	
2010/0024017	A1	1/2010	Ashfield et al.	
2010/0051686	A1	3/2010	Obi	
2010/0095351	A1	4/2010	Liu et al.	
2010/0269162	A1	10/2010	Bravo et al.	
2011/0015449	A1	1/2011	Pendleton et al.	
2011/0039237	A1	2/2011	Skare	
2011/0138483	A1	6/2011	Bravo et al.	
2011/0197070	A1	8/2011	Mizrah	
2011/0225647	A1	9/2011	Dilley et al.	
2011/0277024	A1	11/2011	Begley et al.	
2011/0289576	A1	11/2011	Cheng	
2011/0307366	A1	12/2011	Ahuja et al.	
2012/0011066	A1	1/2012	Telle et al.	
2012/0149334	A1	6/2012	Zhang et al.	
2012/0204241	A1	8/2012	Varsavsky et al.	
2012/0264405	A1	10/2012	Bravo et al.	
2012/0272331	A1	10/2012	Lemaster et al.	
2013/0007859	A1	1/2013	Bravo et al.	
2014/0011561	A1	1/2014	Lutnick et al.	
2014/0016634	A1	1/2014	Khan et al.	
2014/0033279	A1	1/2014	Nimashakavi et al.	

FOREIGN PATENT DOCUMENTS

JP	10334048	A	12/1998
JP	10341224	A	12/1998
JP	2001111545		4/2001
WO	0109808	A1	2/2001
WO	2004079499	A2	9/2004
WO	2006103387	A1	10/2006
WO	2008147353	A1	12/2008

OTHER PUBLICATIONS

Bibbee, U.S. Appl. No. 11/765,193, Office Action Communication, Nov. 29, 2010, 14 pages.

Bibbee, U.S. Appl. No. 11/765,193, Office Action Communication, Jul. 30, 2010, 15 pages.

Bibbee, U.S. Appl. No. 11/765,193, Office Action Communication, Feb. 18, 2010, 15 pages.

Tran, U.S. Appl. No. 11/524,340, Notice of Allowance & Fees Due, Dec. 29, 2009, 11 pages.

Tran, U.S. Appl. No. 11/524,340, Office Action Communication, Jul. 29, 2009, 9 pages.

Tran, U.S. Appl. No. 11/524,340, Office Action Communication, Oct. 31, 2008, 19 pages.

Tran, U.S. Appl. No. 11/524,340, Office Action Communication, May 27, 2008, 22 pages.

Tran, U.S. Appl. No. 11/524,340, Office Action Communication, Apr. 29, 2009, 7 pages.

Bibbee, U.S. Appl. No. 11/765,193, Examiner's Answer, Apr. 16, 2013, 20 pages.

Almeida, U.S. Appl. No. 12/630,875, Office Action, Apr. 17, 2013, 40 pages.

(56) **References Cited**

OTHER PUBLICATIONS

Lakhia, U.S. Appl. No. 11/753,673, Notice of Allowance, Jun. 18, 2012, 11 pages.
Gee, U.S. Appl. No. 13/084,823, Office Action, IBMC-0395, Mar. 11, 2013, 8 pages.
Leung, "Depress Phishing by CAPTCHA with OTP", Department of Information Engineering The Chinese University of Hong Kong, IEEE 2009, 6 pgs.
Kopsidas et al., "Voice Interactive Personalized Security (VoIPSEC) protocol: Fortify Internet telephony by providing end-to-end security through inbound key exchange and biometric verification", 2006 IEEE, 10 pgs.
Koo et al., "VoIP Interception in P2P SIP Environment", 2010 Ieeee, vol. 1, pp. 331-334.
Megeed, U.S. Appl. No. 12/423,928, Office Action 1, IBMC-0326, 21 pages, Aug. 25, 2011.
Megeed, U.S. Appl. No. 12/423,928, Final Office Action 1, IBMC-0326, 20 pages, Nov. 10, 2011.
Megeed, U.S. Appl. No. 12/423,928, Office Action 2, IBMC-0326, 20 pages, Jun. 8, 2012.
Megeed, U.S. Appl. No. 12/423,928, Notice of Allowance 1, IBMC-0326, 10 pages, Sep. 25, 2012.
Megeed, U.S. Appl. No. 12/423,928, Notice of Allowance 2, IBMC-0326, 19 pages, Dec. 4, 2012.
Lakhia, U.S. Appl. No. 13/432,956, Office Action, Feb. 14, 2013, 26 pages.
Lakhia, U.S. Appl. No. 11/753,673, Office Action, Jan. 8, 2013, 14 pages.
Bibbee, U.S. Appl. No. 11/765,193, Office Action 3, 18 pages, Sep. 19, 2011.
Almeida, U.S. Appl. No. 12/630,875, Notice of Allowance, IBMC-0353, Dec. 20, 2012, 7 pages.
Bibbee, U.S. Appl. No. 11/765,193, Final Office Action 2, 17 pages, May 12, 2011.
Bibbee, U.S. Appl. No. 11/765,193, Final Office Action 3, 18 pages, Apr. 16, 2012.
Almeida, U.S. Appl. No. 12/630,875, Office Action, IBMC-0353, Aug. 30, 2012, 14 pages.
Almeida, U.S. Appl. No. 12/630,875, Office Action, IBMC-0353, Mar. 1, 2012, 17 pages.
Geneiatakis et al., "Survey of Security Vulnerabilities in Session Initiation Protocol", 3rd Quarter 2006, vol. 8, No. 3, IEEE Communications Surveys & Tutorials, pp. 68-81.
Bonzo, U.S. Appl. No. 11/776,619, Office Action, Sep. 30, 2009, 12 pages.
Bonzo, U.S. Appl. No. 11/776,619, Notice of Allowance, Apr. 29, 2010, 10 pages.
Alicherry et al., "DoubleCheck: Multi-ath Verification Against Man-in-the-Middle Attack", IEEE 2009, pp. 557-563.
Kumaraguru et al., "Getting Users to Pay Attention to Anti-Phishing Education: Evaluation of Retention and Transfer", APWG eCrime Researchers Summit, Oct. 4-5, 2007, Pittsburgh, PA pp. 70-81.
Adida, "BeamAuth: Two-Factor Web Authentication with a Bookmark", CCS '07, Oct. 29-Nov. 2, 2007, Alexandria, VA, ACM 978-1-59593-703-2/07/0010, pp. 48-57.
Nassar et al., "Holistic VoIP Intrusion Detection and Prevention System", IPTCOMM '07, ACM 2007, pp. 1-9.
Stoll et al., "Sesame: Informing User Security Decisions with System Visualization", CHI 2008 Proceedings, Am I Safe, Apr. 5-10, 2008, Florence, Italy, pp. 1045-1054.
Ma et al., "Beyond Blacklists: Learning to Detect Malicious Web Sites from Suspicious URLs", KDD '09, Jul. 28-Jul. 1, 2009, pp. 1245-1253.
Lakhia, U.S. Appl. No. 13/432,956, Notice of Allowance & Fees Due, Apr. 15, 2013, 27 pages.
U.S. Appl. No. 12/630,875, Notice of allowance and Fee(s) Due dated Nov. 18, 2013, IBMC-0353, 19 pages.
Almeida, U.S. Appl. No. 12/630,875, Office Action Communication, Aug. 7, 2013, 15 pages.
Vaughan, U.S. Appl. No. 13/613,502, Office Action Communication, Jul. 18, 2013, 54 pages.
Vaughan, U.S. Appl. No. 12/423,928, Notice of Allowance & Fees Due, Jul. 11, 2013, 25 pages.
Lakhia, U.S. Appl. No. 11/753,673, Notice of Allowance & Fees Due, dated May 10, 2013, 28 pages.
U.S. Appl. No. 13/613,502, Notice of allowance and Fee(s) Due dated Jan. 27, 2014, IBMC-0326-CON, 14 pages.
U.S. Appl. No. 13/562,491, Office Action dated May 5, 2014, 64 pages.

* cited by examiner

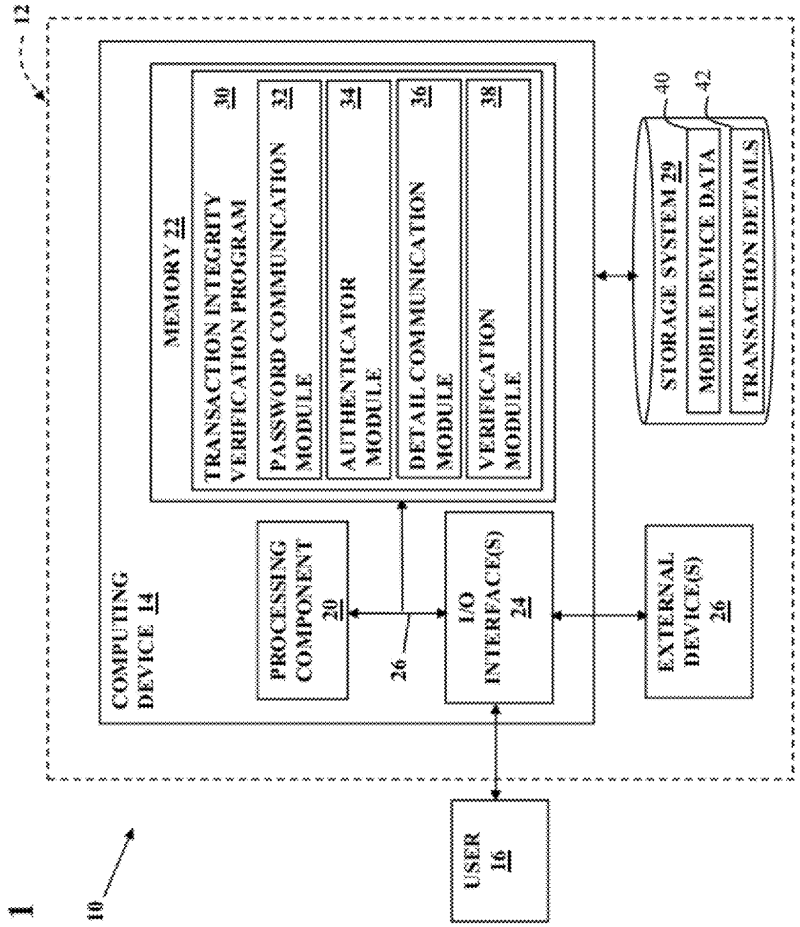

12
COMPUTING DEVICE 14
MEMORY 22
TRANSACTION INTEGRITY VERIFICATION PROGRAM 30
PASSWORD COMMUNICATION MODULE 32
AUTHENTICATOR MODULE 34
DETAIL COMMUNICATION MODULE 36
VERIFICATION MODULE 38
PROCESSING COMPONENT 20
26
I/O INTERFACE(S) 24
EXTERNAL DEVICE(S) 26
40
42
STORAGE SYSTEM 29
MOBILE DEVICE DATA
TRANSACTION DETAILS
USER 16
10

FIG 1

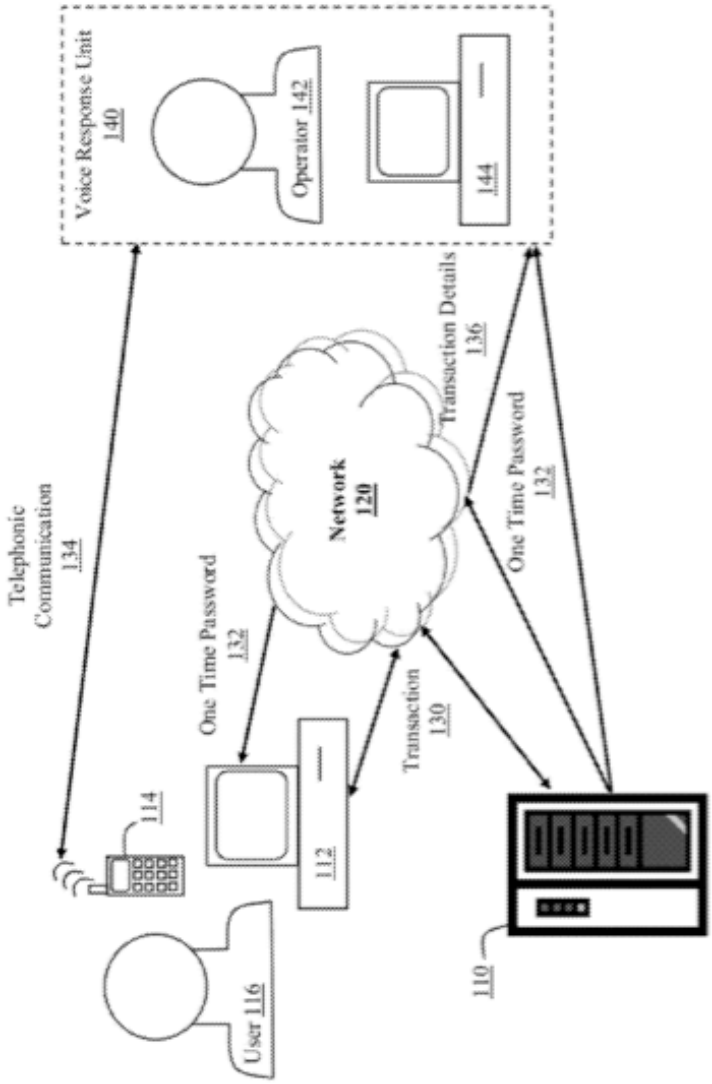

100
Voice Response Unit
140
Operator 142
144
Transaction Details
136
Network
120
One Time Password
132
Telephonic
Communication
134
One Time Password
132
Transaction
130
114
112
User 116
110

FIG 2

VERIFICATION OF TRANSACTIONAL INTEGRITY

REFERENCE TO RELATED APPLICATION

The current application is related to co-owned U.S. Pat. No. 7,715,823 B2, filed on Sep. 20, 2006, and entitled "Methods and Apparatus for Restricting Access of a User Using a Cellular Telephone" and co-owned U.S. Patent Pub. No. 2008/0318548, filed on Jun. 17, 2007, and entitled "Method and System for Strong Authentication and Defense Against Man-in-the-Middle Attacks", each of which is hereby incorporated herein by reference.

FIELD OF THE INVENTION

The subject matter of this invention relates generally to transaction verification. More specifically, aspects of the present invention provide a system and method for verifying the integrity of a commercial transaction.

BACKGROUND OF THE INVENTION

There is an increasing use of electronic media in conducting commercial transactions. These transactions can include such types of transactions as internet banking and electronic commerce, to name a few. However, with the increase of these transactions comes an increased risk that entities without authorization will be able to use the electronic data used in these transactions to benefit themselves and/or harm one or more of the authorized members of the transaction.

Current security solutions attempt to eliminate these unauthorized transactions, but these solutions are deficient with respect to certain type of attack. For example, in one particular type of man-in-the-middle (MITM) type attack, an unauthorized computer program (malware) that has been covertly loaded on a user's computer system or elsewhere along the chain of the transaction could be used to alter the details of a transaction after it has been approved by the user. For example, the malware could alter the details of an online banking transaction that authorized payment of $100 to the electric company in such a way that the new transaction paid $10,000 to the entity that circulated the malware.

SUMMARY OF THE INVENTION

In general, aspects of the present invention provide a solution for verifying the integrity of a transaction. In response to receipt of a confirmed electronic transaction from a user, a one time password is forwarded to the user. The user then initiates a telephonic communication with a verifier on the user's wireless device and provides the one time password to the verifier. The verifier authenticates the mobile telephonic device based on the device's caller identification number and determines whether the one time password provided by the user matches the one forwarded to the user. After the user is authenticated, the verifier communicates the details of the transaction that were received and the user confirms whether the details match those originally entered.

A first aspect of the invention provides a system for verifying the integrity of a transaction, comprising: a password communication module that forwards a one time password to a user upon receipt of a confirmed electronic transaction from the user; an authenticator module that, in response to a telephonic communication from the user regarding the transaction, authenticates a mobile telephonic device used to initiate the telephonic communication based on a caller identification

of the mobile telephonic device and authenticates an inputted one time password entered by the user via the telephonic communication based on the forwarded one time password; a detail communication module that facilitates communication of details of the confirmed electronic transaction to the user via the telephonic communication based on the authentication; and a verification module that verifies the transaction based on an indication via the telephonic communication from the user as to whether the details match originally sent details from the user.

A second aspect of the invention provides a method for verifying the integrity of a transaction, comprising: forwarding, upon receipt of a confirmed electronic transaction from a user, a one time password to the user; receiving a telephonic communication from a mobile telephonic device of the user; authenticating the mobile telephonic device as being associated with the user using a caller identification number of the mobile telephonic device; receiving an input of the one time password from the user via the telephonic communication; authenticating an identity of the user based on a comparison of the input one time password with the forwarded one time password; communicating, based on the authenticating, details of the confirmed electronic transaction to the user via the telephonic communication; and verifying the transaction based on an indication via the telephonic communication from the user as to whether the details match originally sent details from the user.

A third aspect of the invention provides a computer program product embodied in a computer readable medium for implementing a method for verifying the integrity of a transaction, the method comprising: forwarding, upon receipt of a confirmed electronic transaction from a user, a one time password to the user; receiving a telephonic communication from a mobile telephonic device of the user; authenticating the mobile telephonic device as being associated with the user using a caller identification number of the mobile telephonic device; receiving an input of the one time password from the user via the telephonic communication; authenticating an identity of the user based on a comparison of the input one time password with the forwarded one time password; communicating, based on the authenticating, details of the confirmed electronic transaction to the user via the telephonic communication; and verifying the transaction based on an indication via the telephonic communication from the user as to whether the details match originally sent details from the user.

A fourth aspect of the present invention provides a method for deploying an application for verifying the integrity of a transaction, comprising, providing a computer system operable to: forward, upon receipt of a confirmed electronic transaction from a user, a one time password to the user; receive a telephonic communication from a mobile telephonic device of the user; authenticate the mobile telephonic device as being associated with the user using a caller identification number of the mobile telephonic device; receive an input of the one time password from the user via the telephonic communication; authenticate an identity of the user based on a comparison of the input one time password with the forwarded one time password; communicate, based on the authenticating, details of the confirmed electronic transaction to the user via the telephonic communication; and verify the transaction based on an indication via the telephonic communication from the user as to whether the details match originally sent details from the user.

Still yet, any of the components of the present invention could be deployed, managed, serviced, etc., by a service provider who offers to control electricity to a device.

Embodiments of the present invention also provide related systems, methods and/or program products.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other features of this invention will be more readily understood from the following detailed description of the various aspects of the invention taken in conjunction with the accompanying drawings in which:

FIG. **1** shows a data processing system suitable for implementing an embodiment of the present invention.

FIG. **2** shows an environment in which transaction integrity is verified according to an embodiment of the present invention.

The drawings are not necessarily to scale. The drawings are merely schematic representations, not intended to portray specific parameters of the invention. The drawings are intended to depict only typical embodiments of the invention, and therefore should not be considered as limiting the scope of the invention. In the drawings, like numbering represents like elements.

DETAILED DESCRIPTION OF THE INVENTION

As indicated above, aspects of the present invention provide a solution for verifying the integrity of a transaction. In response to receipt of a confirmed electronic transaction from a user, a one time password is forwarded to the user. The user then initiates a telephonic communication with a verifier on the user's wireless device and provides the one time password to the verifier. The verifier authenticates the mobile telephonic device based on the device's caller identification number and determines whether the one time password provided by the user matches the one forwarded to the user. After the user is authenticated, the verifier communicates the details of the transaction that were received and the user confirms whether the details match those originally entered.

As a result, the current invention provides greater security for electronic transactions. Specifically, the verification of the details of the transaction by the user provides greater security than those provided by simple provider-based assess verification systems currently in existence. This verification as part of the current invention foils man-in-the-middle (MITM) attacks that would have otherwise succeeded under previous solutions.

Turning to the drawings, FIG. **1** shows an illustrative environment **10** for verifying the integrity of a transaction according to an embodiment. To this extent, environment **10** includes a computer system **12** that can perform a process described herein in order to verify the integrity of a transaction. In particular, computer system **12** is shown including a computing device **14** that includes a transaction integrity verification program **30**, which makes computing device **14** operable to verify the integrity of a transaction by performing a process described herein.

Computing device **14** is shown including a processing component **20** (e.g., one or more processors), a memory **22**, a storage system **29** (e.g., a storage hierarchy), an input/output (I/O) interface component **24** (e.g., one or more I/O interfaces and/or devices), and a communications pathway **26**. In general, processing component **20** executes program code, such as transaction integrity verification program **30**, which is at least partially fixed in memory **22**. While executing program code, processing component **20** can process data, which can result in reading and/or writing transformed data from/to memory **22** and/or I/O interface component **24** for further processing. Pathway **26** provides a communications link between each of the components in computer system **12**. I/O interface component **24** can comprise one or more peripheral I/O devices, which enable communications with an external device **26**. Additionally, or in the alternative, I/O interface component **24** can comprise one or more human I/O devices, which enable a human user **16** to interact with computer system **12** and/or one or more communications devices to enable a system user **16** to communicate with computer system **12** using any type of communications link. To this extent, transaction integrity verification program **30** can manage a set of interfaces (e.g., graphical user interface(s), application program interface, and/or the like) that enable human and/or system users **16** to interact with transaction integrity verification program **30**. Further, transaction integrity verification program **30** can manage (e.g., store, retrieve, create, manipulate, organize, present, etc.) the data, such as mobile device data **40** and/or transaction details **42**, using any solution.

In any event, computer system **12** can comprise one or more general purpose computing articles of manufacture **14** (e.g., computing devices) capable of executing program code, such as transaction integrity verification program **30**, installed thereon. As used herein, it is understood that "program code" means any collection of instructions, in any language, code or notation, that cause a computing device having an information processing capability to perform a particular action either directly or after any combination of the following: (a) conversion to another language, code or notation; (b) reproduction in a different material form; and/or (c) decompression. To this extent, transaction integrity verification program **30** can be embodied as any combination of system software and/or application software. In any event, the technical effect of computer system **12** is to provide processing instructions to computing device **14** in order to verify the integrity of a transaction.

Further, transaction integrity verification program **30** can be implemented using a set of modules **32-38**. In this case, a module **32-38** can enable computer system **12** to perform a set of tasks used by transaction integrity verification program **30**, and can be separately developed and/or implemented apart from other portions of transaction integrity verification program **30**. As used herein, the term "component" means any configuration of hardware, with or without software, which implements the functionality described in conjunction therewith using any solution, while the term "module" means program code that enables a computer system **12** to implement the actions described in conjunction therewith using any solution. When fixed in a memory **22** of a computer system **12** that includes a processing component **20**, a module is a substantial portion of a component that implements the actions. Regardless, it is understood that two or more components, modules, and/or systems may share some/all of their respective hardware and/or software. Further, it is understood that some of the functionality discussed herein may not be implemented or additional functionality may be included as part of computer system **12**.

When computer system **12** comprises multiple computing devices **14**, each computing device can have only a portion of transaction integrity verification program **30** fixed thereon (e.g., one or more modules **32-38**). However, it is understood that computer system **12** and transaction integrity verification program **30** are only representative of various possible equivalent computer systems that may perform a process described herein. To this extent, in other embodiments, the functionality provided by computer system **12** and transaction integrity verification program **30** can be at least partially implemented by one or more computing devices that include any combination of general and/or specific purpose hardware

with or without program code. In each embodiment, the hardware and program code, if included, can be created using standard engineering and programming techniques, respectively.

Regardless, when computer system **12** includes multiple computing devices **14**, the computing devices can communicate over any type of communications link. Further, while performing a process described herein, computer system **12** can communicate with one or more other computer systems using any type of communications link. In either case, the communications link can comprise any combination of various types of wired and/or wireless links; comprise any combination of one or more types of networks; and/or utilize any combination of various types of transmission techniques and protocols.

As discussed herein, transaction integrity verification program **30** enables computer system **20** to verify the integrity of a transaction. To this extent, transaction integrity verification program **30** is shown including a password communication module **32**, an authenticator module **34**, a detail communication module **36**, and a verification module **38**.

Referring now to FIG. **2**, an environment **100**, in which the integrity of a transaction **130** can be verified, is shown. As shown, environment **100** includes a user **116**, having both a computer transaction device **112** for conducting transaction **130** and a mobile telephonic device **114** for initiating a telephonic communication **134**. User **116** communicates with a transaction partner **110** over a network **120**. Transaction partner **110** can include any combination of hardware, software, etc., now known or later developed that is capable of carrying out transaction **130** with user **116**, including, but not limited to a transaction **130** involving online banking, electronic commerce, etc. Network **120** can include any network for carrying data, such as transaction **130**, including wired, wireless, internet, intranet, etc. Further, while computer transaction device **112** and mobile telephonic device **114** are shown as being different devices, it should be understood by those skilled in the art, that the functions of computer transaction device **112** and mobile telephonic device **114** could be performed by the same device. For example, this could occur in the case that mobile telephonic device **114** also had computational features, including, but not limited to network access features that allowed mobile telephonic device **114** to communicate over a network **120** to perform a transaction **130**.

Environment **100** also includes a voice response unit **140** that verifies the integrity of transaction **130**. As shown, voice response unit **140** includes an operator **142** and a verification computer device **144** that enables operator **142** to verify the integrity of transaction **130**. Voice response unit **140** can be, as illustrated, a third party entity that is separate from transaction partner **110**, including, but not limited to a telephone carrier that provides service for mobile telephonic device **114**. In the alternative, voice response unit **140** could be associated with transaction partner **110** in, for example, the same company, location, etc. While environment **100**, as illustrated, shows a human operator **142**, it should be understood, that in some embodiments, the functions of operator **142** could be performed by a computer, such as an automated answering service, working in conjunction with verification computer device **144**.

In any case, referring now to FIG. **1** in conjunction with FIG. **2**, computer system **12** (e.g., password communication module **32**) communicates a one time password **132** to a user **116** upon receipt of electronic transaction **130** that has been completed. Specifically, prior to communication of one time password **132**, user **116** accesses transaction partner **110** using computer transaction device **112** over network **120**. This access can be performed by any solution now known or later developed for a device to establish a communication with another device, including but not limited to, a web page, a web portal, an electronic mail message, a dedicated pipeline, etc. In any case, user **116** can establish user's **116** identity with transaction partner **110** with a login or other known solution, and user **116** can communicate with transaction partner **110** to provide transaction partner **110** with details of transaction **130**. For example, if transaction **110** is a banking transaction to pay a bill of user **116**, user **116** could specify an amount for payment (e.g., $100) and information indicating to whom the payment should be made (e.g., WOW Electric). Details of transaction **130** could have any number of items and could include any items that can be used to facilitate a transaction, such as transaction amount, transaction destination, transaction source account, transaction destination account, transaction source institution, transaction currency used, transaction date, etc.

In any event, after the details have been entered by user **116**, user **116** will communicate the details to transaction partner **110** along with a confirmation for processing transaction **130**. In response, transaction partner **110** communicates one time password **132** to user **116** via network **120**. One time password **132** is unique to transaction **130**. As such, one time password **132** can only be used to verify the particular transaction **130** for the particular user **116** to which transaction partner **110** has communicated it. In one environment, one time password **132** is an alphabetic, numeric, or alphanumeric string, although other embodiments are envisioned. Transaction partner **110** can also forward a telephonic identifier to user **116** that user **116** can use to contact voice response unit **140**. This telephonic identifier could be a standard telephone number having 7, 10 or other standard number of digits. In the alternative, the telephonic identifier could a mobile telephone carrier based service message. In this case, a number, which is often preceded by a character, such as "*" or "#" is routed directly by the telephone carrier that user **116** uses in conjunction with mobile telephonic device **114** to a predetermined location associated with voice response unit **140**.

Transaction partner **110** also, upon receipt of the confirmed transaction **130**, can forward one time password **132** and transaction details **136** of the confirmed transaction **130** to voice response unit **140**. As shown, one time password **132** and/or transaction details **136** could be communicated to voice response unit **140** over network **120**, or, in the alternative one or both could be communicated by an alternate solution, such as an internal network, dedicated connection between transaction partner **110** and voice response unit **140**, or other secure manner of communication. It should be understood the one time password **132** that is communicated from transaction partner **110** to voice response unit **140** corresponds to one time password **132** that has been communicated to user **116**. To this extent, each of the one time passwords **132** associated with transaction **130** could be identical. In the alternative, the one time password **132** forwarded to user **116** could include a key that decrypts the one time password **132** forwarded to voice response unit **140**, or vice versa. It should also be understood that in most cases transaction details forwarded from transaction partner **110** to voice response unit **140** would match the details of transaction **130** communicated from user **116** to transaction partner **110**. However, in the case that the details of transaction **130** have been altered subsequent to confirmation by user **116** but prior to receipt by transaction partner **110**, the details will be different from

transaction details **136** received by transaction partner **110** and forwarded from transaction partner **110** to voice response unit **140**.

Referring still to FIG. **1** in conjunction with FIG. **2**, computer system **12** (e.g., authenticator module **34**) authenticates the identity of user **116** at voice response unit **140**. Specifically, user **116** uses the telephonic identifier previously forwarded to user **116** from transaction partner **110** to initiate telephonic communication **134** with voice response unit **140** using mobile telephonic device **114**. Upon receipt of telephonic communication **134** by voice response unit **140**, authenticator module **34** authenticates mobile telephonic device **114**. This can be accomplished by comparing the caller identification information that identifies the incoming telephone number of mobile telephonic device **114** in telephonic communication **134** with mobile device data **40** that is on record with voice response unit **140**, such as in mobile device data **42** of storage system **29** (FIG. **1**), as being associated with user **116**. The fact that mobile telephonic device **114** is a mobile device (e.g., a cellular telephone) makes the authentication of telephonic communication **134** as originating with user **116** that is performed by authenticator module **34** more accurate. This is because it is currently more difficult to spoof, or impersonate the identity of a caller when the telephonic device is a mobile phone than when it is a land line. Furthermore, the fact that mobile telephonic device **114** is unique to user **116** and carried by user **116** makes mobile telephonic device a more secure source of authentication that a land line, which can often be shared. In addition the portability associated with mobile telephonic device provides added convenience to user **116** during the validation process.

Authenticator module **34** can then authenticate user **116** on a transaction **130** level using one time password **132**. To accomplish this, user **116** can be prompted to enter the one time password **132** that transaction partner **110** previously sent to user **116** upon confirmation of transaction **130**. Authenticator module **34** can then compare the input one time password **132** with the one time password that was sent from transaction partner **110** to voice response unit **140**. If the one time password **132** provided by user **116** corresponds to the one time password sent from transaction partner **110**, voice response unit **140** can authenticate user **116** for transaction **130**.

Once user **116** is authenticated, computer system **12** (e.g., detail communication module **36**) facilitates communication of transaction details **136** of confirmed transaction **130** to user **116** on mobile telephonic device **114** via telephonic communication **134**. To accomplish this, voice response unit **140** can access stored transaction details **136** that were previously communicated to voice response unit **140** from transaction partner **110** and stored. These transaction details **136** can be retrieved using verification computer device **144**, by searching stored transaction details **42** using one time password **132** as a key. Once retrieved by voice response unit **140**, transaction details **136** can be communicated to user **116** by a human operator **142**, or, in the alternative, by a computerized operator **142** utilizing a speech simulator to convert stored transaction details **42** to speech and communicating transaction details **136** to mobile telephonic device **114** of user **116** over telephonic communication **134**. In an alternative embodiment, detail communication module **36** can receive a communication from user **116** over telephonic communication **134** that reiterates transaction details **136** of transaction **130** rather than voice response unit **140** communicating stored transaction details **42** to user **116**.

After transaction details **136** have been communicated, computer system **12** (e.g., verification module **38**) verifies the integrity of confirmed transaction **130**. A comparison is made over telephonic communication **134** between transaction details **136** from user **116** and stored transaction details **42** that have been sent from transaction partner **110** to voice response unit **140**. Based on the comparison, an indication can be made as to whether stored details **42** match transaction details **136** originally received from user **116**. In an embodiment in which stored transaction details **42** have been communicated to user **116**, it could be user **116** that performs the verification and makes the indication to voice response unit **140**. In the alternative, in the case that user **116** communicates transaction details **136** to voice response unit **140**, voice response unit **140** could perform the verification and make the indication. Furthermore, in either embodiment, the verification and indication could be performed by a combination of user **116** and voice response unit **140**.

For example, assume original transaction details **136** include:

Pay from bank account;
Amount of $100; and
To WOW Energy.

Then, if transaction **130** has not been altered, stored transaction details **42** will match original transaction details **136** and there will be an indication from verification module **38** to that effect. This indication could be made by user **116** and/or operator **140** via telephonic communication **134**. Based on the indication, verification module **38** could complete the transaction.

However, if, in the alternative, stored transaction details **42** are as follows:

Transfer from bank account;
Amount of $10,000; and
To Nefarian Co,

then the indication from verification module **38** would be that there is no match. In this case, the details of transaction **130** have been altered subsequent to confirmation by user **116** but prior to receipt by transaction partner **110**. Thus, the details will be different from transaction details **136** received by transaction partner **110** and forwarded from transaction partner **110** to voice response unit **140**. User **116** could be given the opportunity to abort the transaction (such as by pressing the digit 1 to cancel via telephonic communication **134**, for example). It could then be deduced from this indication that data had been modified by a MITM attack, transaction **130** could be aborted, and further investigation as to the source could be conducted.

While shown and described herein as a method and system for verifying the integrity of a transaction, it is understood that aspects of the invention further provide various alternative embodiments. For example, in one embodiment, the invention provides a computer program fixed in at least one computer-readable medium, which when executed, enables a computer system to verify the integrity of a transaction. To this extent, the computer-readable medium includes program code, such as transaction integrity verification program **30** (FIG. **1**), which implements some or all of a process described herein. It is understood that the term "computer-readable medium" comprises one or more of any type of tangible medium of expression, now known or later developed, from which a copy of the program code can be perceived, reproduced, or otherwise communicated by a computing device. For example, the computer-readable medium can comprise: one or more portable storage articles of manufacture; one or more memory/storage components of a computing device; paper; and/or the like.

In another embodiment, the invention provides a method of providing a copy of program code, such as transaction integ-

rity verification program **30** (FIG. **1**), which implements some or all of a process described herein. In this case, a computer system can process a copy of program code that implements some or all of a process described herein to generate and transmit, for reception at a second, distinct location, a set of data signals that has one or more of its characteristics set and/or changed in such a manner as to encode a copy of the program code in the set of data signals. Similarly, an embodiment of the invention provides a method of acquiring a copy of program code that implements some or all of a process described herein, which includes a computer system receiving the set of data signals described herein, and translating the set of data signals into a copy of the computer program fixed in at least one computer-readable medium. In either case, the set of data signals can be transmitted/received using any type of communications link.

In still another embodiment, the invention provides a method of generating a system for verifying the integrity of a transaction. In this case, a computer system, such as computer system **12** (FIG. **1**), can be obtained (e.g., created, maintained, made available, etc.) and one or more components for performing a process described herein can be obtained (e.g., created, purchased, used, modified, etc.) and deployed to the computer system. To this extent, the deployment can comprise one or more of: (1) installing program code on a computing device; (2) adding one or more computing and/or I/O devices to the computer system; (3) incorporating and/or modifying the computer system to enable it to perform a process described herein; and/or the like.

The terms "first," "second," and the like, herein do not denote any order, quantity, or importance, but rather are used to distinguish one element from another, and the terms "a" and "an" herein do not denote a limitation of quantity, but rather denote the presence of at least one of the referenced item. The modifier "approximately" used in connection with a quantity is inclusive of the stated value and has the meaning dictated by the context, (e.g., includes the degree of error associated with measurement of the particular quantity). The suffix "(s)" as used herein is intended to include both the singular and the plural of the term that it modifies, thereby including one or more of that term (e.g., the metal(s) includes one or more metals). Ranges disclosed herein are inclusive and independently combinable (e.g., ranges of "up to approximately 25 wt %, or, more specifically, approximately 5 wt % to approximately 20 wt %", is inclusive of the endpoints and all intermediate values of the ranges of "approximately 5 wt % to approximately 25 wt %," etc).

The foregoing description of various aspects of the invention has been presented for purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise form disclosed, and obviously, many modifications and variations are possible. Such modifications and variations that may be apparent to an individual in the art are included within the scope of the invention as defined by the accompanying claims.

We claim:

1. A system for preventing man-in-the-middle (MITM) attacks, the system comprising at least one computer device that performs a method comprising:

forwarding a transaction-specific onetime password and a telephonic identifier to a user upon receipt of a confirmed electronic transaction from the user, wherein the telephonic identifier includes an authentication telephone number routed directly to a predetermined location;

storing a set of confirmed details for the transaction, wherein the set of confirmed details includes the transaction-specific onetime password, a confirmed transaction source, and a confirmed transaction destination;

in response to a telephonic communication from the user regarding the transaction, authenticating a mobile telephonic device used to initiate the telephonic communication based on a caller identification of the mobile telephonic device and the telephonic identifier;

authenticating an inputted one time password entered by the user via the telephonic communication based on the forwarded transaction-specific onetime password;

facilitating verbal communication of user-submitted details of the confirmed electronic transaction from the user via the telephonic communication based on the authentication, wherein the user-submitted details include a submitted transaction source and a submitted transaction destination;

identifying the set of confirmed details for the transaction by reference to the transaction-specific onetime password; and

verifying the transaction based on an indication via the telephonic communication and the verbal communication from the user as to whether the user-submitted details from the user match the confirmed details for the transaction.

2. The system of claim **1**, the method further comprising the electronic transaction if the indication is that the details match, and aborting the electronic transaction if the indication is that the details do not match.

3. The system of claim **1**, wherein the telephonic communication is performed using a mobile telephonic carrier-based service message.

4. The system of claim **1**, wherein the authenticating is performed by a third party who is not a participant in the electronic transaction.

5. The system of claim **1**, wherein the electronic transaction is selected from the group comprising: an online banking transaction or an electronic commerce transaction.

6. The system of claim **1**, wherein the forwarded one time password further comprises a decryption key, and the comparison of the input one time password with the forwarded one time password includes decrypting the input one time password.

7. The system of claim **1**, wherein the verifying is performed using a voice response unit having an operator and a verification computer device.

8. The system of claim **1**, wherein the facilitating includes verbal communication of details of the confirmed electronic transaction both from the user and to the user via the telephonic communication based on the authentication, and the verifying is based on the indication via the telephonic transaction and the verbal communication of details of the conformed electronic transaction both from the user and to the user.

9. A method for preventing man-in-the-middle (MITM) attacks, the method comprising:

forwarding, upon receipt of a confirmed electronic transaction from a user, a transaction-specific onetime password and a telephonic identifier to the user, wherein the telephonic identifier includes an authentication telephone number routed directly to a predetermined location;

storing a set of confirmed details for the transaction, wherein the set of confirmed details includes the transaction-specific onetime password, a confirmed transaction source, and a confirmed transaction destination;

receiving a telephonic communication from a mobile telephonic device of the user;

authenticating the mobile telephonic device as calling the authentication telephone number and being associated with the user using a caller identification number of the mobile telephonic device;

receiving an input of the transaction-specific onetime password from the user via the telephonic communication;

authenticating an identity of the user based on a comparison of the input one time password with the forwarded one time password;

receiving a verbal communication from the user of user-submitted details of the confirmed electronic transaction via the telephonic communication, wherein the user-submitted details include a submitted transaction source and a submitted transaction destination;

identifying the set of confirmed details for the transaction by reference to the transaction-specific onetime password; and

verifying the transaction based on an indication via the telephonic communication and the verbal communication from the user as to whether the user-submitted details match the confirmed details for the transaction.

10. The method of claim **9**, wherein the electronic transaction is completed if the indication is that the details match, and wherein the electronic transaction is aborted if the indication is that the details do not match.

11. The method of claim **9**, wherein the telephonic communication is performed using a mobile telephonic carrier-based service message.

12. The method of claim **9**, wherein the authenticating is performed by a third party who is not a participant in the electronic transaction.

13. The method of claim **9**, wherein the electronic transaction is selected from the group comprising: an online banking transaction or an electronic commerce transaction.

14. The method of claim **9**, wherein the forwarded one time password further comprises a decryption key, and the comparison of the input one time password with the forwarded one time password includes decrypting the input one time password.

15. A computer program product embodied in a computer readable storage medium for implementing a method for preventing man-in-the-middle (MITM) attacks, the method comprising:

forwarding, upon receipt of a confirmed electronic transaction from a user, a transaction-specific onetime password and a telephonic identifier to the user, wherein the telephonic identifier includes an authentication telephone number routed directly to a predetermined location;

storing a set of confirmed details for the transaction, wherein the set of confirmed details includes the transaction-specific onetime password, a confirmed transaction source, and a confirmed transaction destination;

receiving a telephonic communication from a mobile telephonic device of the user;

authenticating the mobile telephonic device as calling the authentication telephone number and being associated with the user using a caller identification number of the mobile telephonic device;

receiving an input of the transaction-specific onetime password from the user via the telephonic communication;

authenticating an identity of the user based on a comparison of the input one time password with the forwarded one time password;

receiving a verbal communication from the user of user-submitted details of the confirmed electronic transaction via the telephonic communication, wherein the user-submitted details include a submitted transaction source and a submitted transaction destination;

identifying the set of confirmed details for the transaction by reference to the transaction-specific onetime password; and

verifying the transaction based on an indication via the telephonic communication and the verbal communication from the user as to whether the user-submitted details match the confirmed details for the transaction.

16. The program product of claim **15**, wherein the electronic transaction is completed if the indication is that the details match, and wherein the electronic transaction is aborted if the indication is that the details do not match.

17. The program product of claim **15**, wherein the telephonic communication is performed using a mobile telephonic carrier-based service message.

18. The program product of claim **15**, wherein the authenticating is performed by a third party who is not a participant in the electronic transaction.

19. The program product of claim **15**, wherein the electronic transaction is selected from the group comprising: an online banking transaction or an electronic commerce transaction.

20. The program product of claim **15**, wherein the forwarded one time password further comprises a decryption key, and the comparison of the input one time password with the forwarded one time password includes decrypting the input one time password.

* * * * *

9.6 VERIFYING ONLINE TRANSACTION INTEGRITY AND AUTHENTICATION WITH QR CODES

US010169759B2

(12) **United States Patent**
Bravo et al.

(10) **Patent No.: US 10,169,759 B2**
(45) **Date of Patent: Jan. 1, 2019**

(54) **VERIFYING ONLINE TRANSACTION INTEGRITY AND AUTHENTICATION WITH QR CODES**

(71) Applicant: **International Business Machines Corporation**, Armonk, NY (US)

(72) Inventors: **Jose F. Bravo**, Old Greenwich, CT (US); **Jeffery L. Crume**, Raleigh, NC (US)

(73) Assignee: **International Business Machines Corporation**, Armonk, NY (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 462 days.

(21) Appl. No.: **14/821,924**

(22) Filed: **Aug. 10, 2015**

(65) **Prior Publication Data**

US 2017/0046699 A1 Feb. 16, 2017

(51) **Int. Cl.**

G06Q 40/00	(2012.01)
G06Q 20/40	(2012.01)
G06K 19/06	(2006.01)
G06K 7/14	(2006.01)

(52) **U.S. Cl.**

CPC ***G06Q 20/405*** (2013.01); ***G06K 7/1417*** (2013.01); ***G06K 19/06037*** (2013.01)

(58) **Field of Classification Search**

CPC G06Q 20/405
USPC 705/15, 75
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

7,133,662	B2	11/2006	Bravo et al.
7,715,823	B2	5/2010	Bravo et al.
7,793,155	B2	9/2010	Belvin et al.
8,522,349	B2	8/2013	Crume
8,533,821	B2	9/2013	Crume
8,683,609	B2	3/2014	Bravo et al.
8,762,724	B2	6/2014	Bravo et al.
8,838,988	B2	9/2014	Bravo et al.

(Continued)

FOREIGN PATENT DOCUMENTS

JP	2008152737	A	7/2008
WO	2014122614	A2	8/2014

(Continued)

OTHER PUBLICATIONS

Andrade, Greg; "Choosing the Best and Safest Two-factor Authentication Method"; SecSign Technologies; Sep. 5, 2014; pp. 1-6; <https://www.secsign.com/best-safest-two-factor-authentication-method/>.

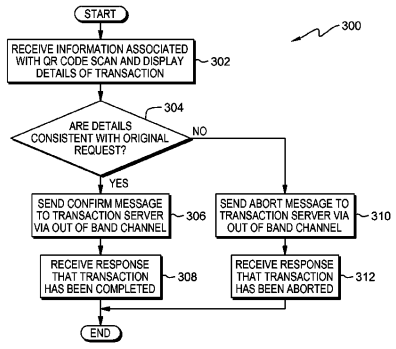
(Continued)

Primary Examiner — Samica L Norman
(74) *Attorney, Agent, or Firm* — Daniel R. Simek

(57) **ABSTRACT**

Embodiments of the present invention provide a method, computer program product, and computer system for verifying transactions over a network. The method includes initiating a proposed transaction with a transaction server. The transaction server provides encoded details of the proposed transaction, in the form of a QR code, to the user. The QR code is scanned using a computing device, and is decoded using an application on the computing device. A set of transaction details associated with the decoded QR code is compared with the details of the proposed transaction. The proposed transaction is then confirmed or aborted using a separate communication channel.

20 Claims, 4 Drawing Sheets



(56) **References Cited**

U.S. PATENT DOCUMENTS

8,917,826	B2	12/2014	Bravo et al.	
2008/0318548	A1	12/2008	Bravo et al.	
2010/0269162	A1	10/2010	Bravo et al.	
2013/0086650	A1	4/2013	Soundrapandian et al.	
2013/0124425	A1*	5/2013	Agrawal	H04L 9/3247 705/75
2015/0088758	A1	3/2015	Varadarajan et al.	
2015/0178721	A1*	6/2015	Pandiarajan	G06Q 20/382 705/75
2016/0063473	A1*	3/2016	Lee	G06Q 30/0633 705/15
2017/0039559	A1*	2/2017	Frieden	G06Q 20/40

FOREIGN PATENT DOCUMENTS

WO	2015014383	A1	2/2015
WO	2015031843	A1	3/2015

OTHER PUBLICATIONS

Shamal et al.; "Secure Authentication for Online Banking Using QR Code"; International Journal of Emerging Technology and Advanced Engineering; Mar. 2014; pp. 778-781; vol. 4; Issue 3.

* cited by examiner

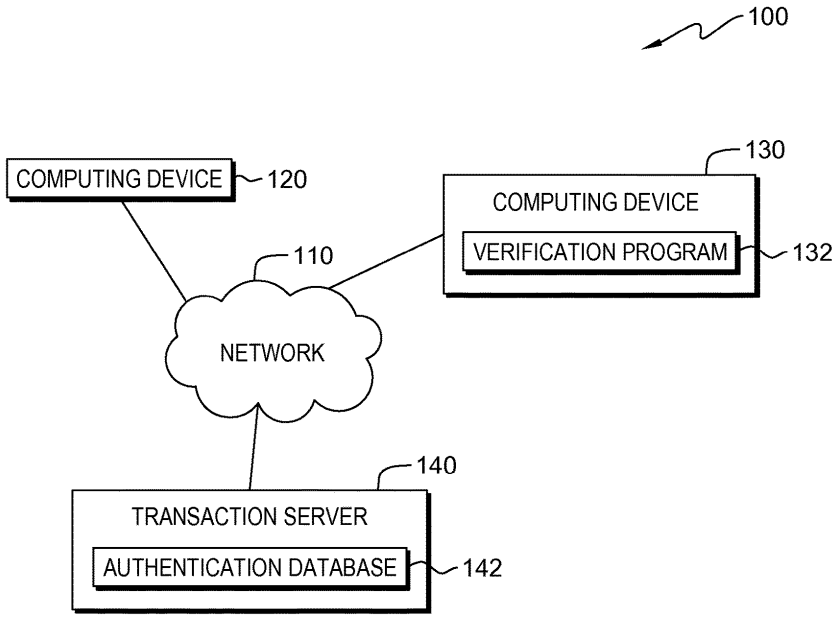

100
COMPUTING DEVICE
120
130
COMPUTING DEVICE
VERIFICATION PROGRAM
132
110
NETWORK
140
TRANSACTION SERVER
AUTHENTICATION DATABASE
142

FIG. 1

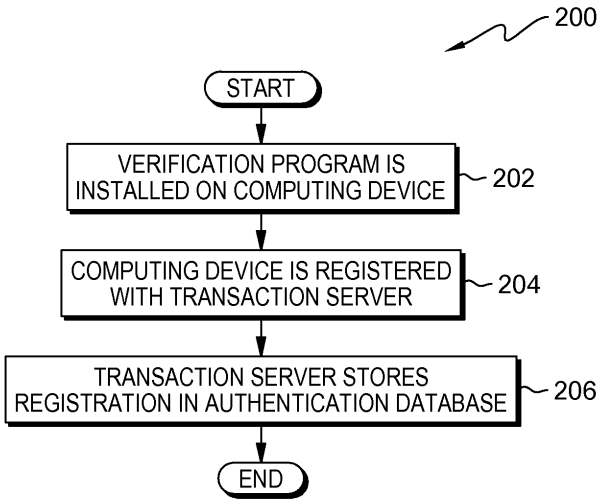

200
START
VERIFICATION PROGRAM IS INSTALLED ON COMPUTING DEVICE
202
COMPUTING DEVICE IS REGISTERED WITH TRANSACTION SERVER
204
TRANSACTION SERVER STORES REGISTRATION IN AUTHENTICATION DATABASE
206
END

FIG. 2

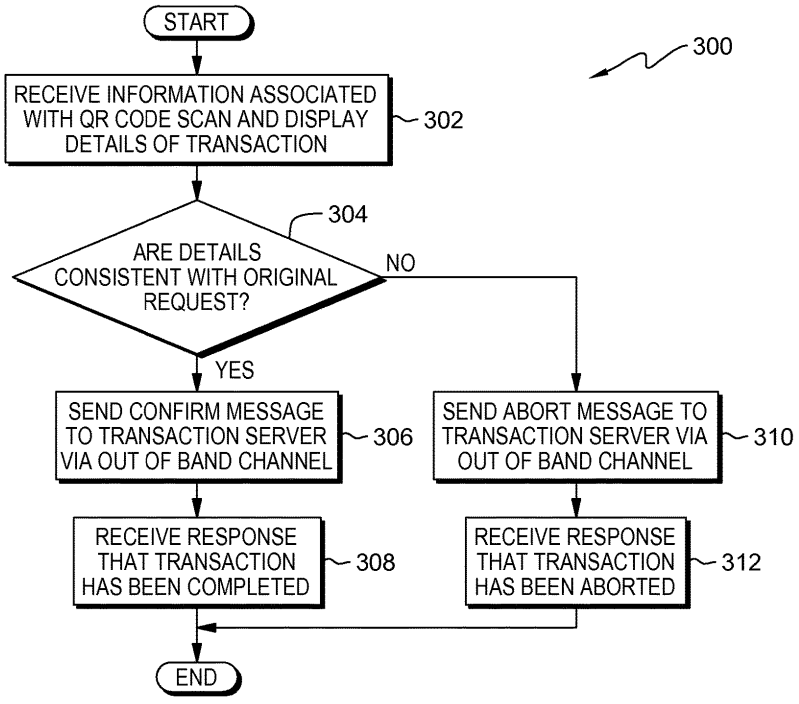

START
300
RECEIVE INFORMATION ASSOCIATED WITH QR CODE SCAN AND DISPLAY DETAILS OF TRANSACTION
302
304
ARE DETAILS CONSISTENT WITH ORIGINAL REQUEST?
NO
YES
SEND CONFIRM MESSAGE TO TRANSACTION SERVER VIA OUT OF BAND CHANNEL
306
SEND ABORT MESSAGE TO TRANSACTION SERVER VIA OUT OF BAND CHANNEL
310
RECEIVE RESPONSE THAT TRANSACTION HAS BEEN COMPLETED
308
RECEIVE RESPONSE THAT TRANSACTION HAS BEEN ABORTED
312
END

FIG. 3

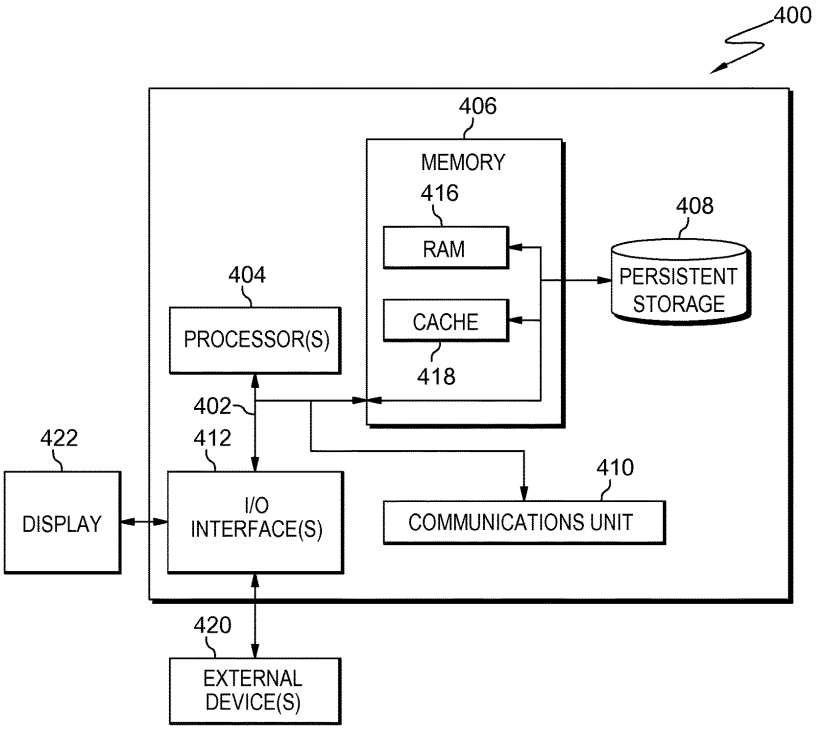

400
406
MEMORY
416
RAM
CACHE
418
408
PERSISTENT STORAGE
404
PROCESSOR(S)
402
412
422
DISPLAY
I/O INTERFACE(S)
410
COMMUNICATIONS UNIT
420
EXTERNAL DEVICE(S)

FIG. 4

VERIFYING ONLINE TRANSACTION INTEGRITY AND AUTHENTICATION WITH QR CODES

BACKGROUND OF THE INVENTION

The present invention relates generally to the field of online transactions, and more particularly to securing the integrity of online transactions using out of band communication.

In cryptography and computer security, a man-in-the-middle (MITM) attack is an attack where the attacker secretly relays, and possibly alters, the communication between two parties who believe they are directly communicating with each other. One example is active eavesdropping, in which the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.

Quick Response (QR) Codes are a type of matrix barcode (or two-dimensional barcode). A barcode is a machine-readable optical label that contains information about the item to which it is attached. A QR code uses four standardized encoding modes (numeric, alphanumeric, byte/binary, and kanji) to efficiently store data; extensions may also be used. The QR Code system has become popular due to its fast readability and greater storage capacity compared to standard Universal Product Code (UPC) barcodes. Applications include product tracking, item identification, time tracking, document management, and general marketing. A QR code consists of black modules (square dots) arranged in a square grid on a white background, which can be read by an imaging device (such as a camera) and processed using Reed-Solomon error correction until the image can be appropriately interpreted. The required data are then extracted from patterns present in both horizontal and vertical components of the image.

SUMMARY

A method, computer program product, and computer system for verifying transactions over a network are provided, comprising: providing, by a registered user, details of a proposed transaction to a transaction server; providing, by the transaction server, to the registered user, a QR code, wherein the QR code comprises encoded details of the proposed transaction; scanning, by a first computing device, the QR code; decoding, by an application of the first computing device, the QR code; comparing, by one or more computer processors, a set of transaction details associated with the decoded QR code to the details of the proposed transaction; and confirming, by a separate communication channel, the proposed transaction.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a functional block diagram illustrating an online transaction verification environment, in accordance with an embodiment of the present invention;

FIG. **2** is a flowchart depicting operational steps for setting up an online transaction verification program, in accordance with an embodiment of the present invention;

FIG. **3** is a flowchart depicting operational steps for verifying online transaction integrity and authentication, in accordance with an embodiment of the present invention; and

FIG. **4** is a block diagram of internal and external components of a computing device, in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION

Online transactions may be at risk of tampering due to the actions of a man-in-the-middle (MITM), who is positioned between the user and the transaction server. In such a scenario, the server believes it is communicating directly with the user and the user directly with the server. However, both parties are actually interacting with the MITM, who is intercepting and potentially modifying details of the transaction. Embodiments of the present invention provide systems and methods for a user to verify transaction details using Quick Response (QR) codes that exposes tampering by an MITM.

The present invention will now be described in detail with reference to the figures. FIG. **1** is a functional block diagram illustrating an online transaction verification environment, generally designated **100**, in accordance with one embodiment of the present invention. FIG. **1** provides only an illustration of one implementation, and does not imply any limitations with regard to the environments in which different embodiments may be implemented. Many modifications to the depicted environment may be made by those skilled in the art without departing from the scope of the invention as recited by the claims. In an exemplary embodiment, online transaction verification environment **100** includes computing device **120** and computing device **130** connected to transaction server **140** over network **110**.

Network **110** can be, for example, a local area network (LAN), a wide area network (WAN) such as the Internet, or a combination of the two, and can include wired, wireless, or fiber optic connections. In general, network **110** can be any combination of connections and protocols that will support communication between transaction server **140** and computing devices **120** and **130**.

Computing device **120** and computing device **130** may be a computing device, such as a laptop computer, a tablet computer, a netbook computer, a personal computer (PC), a desktop computer, a personal digital assistant (PDA), a smart phone or wearable device, a thin client, or any programmable electronic device capable of communicating with transaction server **140** via network **110**. In other embodiments, computing device **120** and computing device **130** may be a management server, a web server, or any other electronic device or computing system capable of receiving and sending data. Computing device **120** and computing device **130** may include internal and external hardware components, as depicted and described in further detail with respect to FIG. **4**. In this exemplary embodiment, computing device **120** includes a web browser capable of displaying a QR code. In another embodiment, computing device **120** is an automated teller machine (ATM) capable of displaying a QR code.

Computing device **130** includes verification program **132** and is pre-registered with transaction server **140**. Transaction server **140** associates a user with a specific computing device **130** and stores this data in authentication database **142**. Verification program **132** is capable of decoding QR codes, presenting the decoded details to the user, and prompting the user to confirm or abort the transaction. In this exemplary embodiment, verification program **132** processes requests from transaction server **140**.

Transaction server **140** sends QR codes to computing device **120** and includes authentication database **142**. Trans-

action server **140** may be a management server, a web server, or any other electronic device or computing system capable of receiving and sending data. In other embodiments of the present invention, transaction server **140** can represent a computing system utilizing clustered computers and components to act as a single pool of seamless resources when accessed through a network. In this exemplary embodiment, transaction server **140** is capable of receiving requests for data from computing device **120** and computing device **130**, via network **110**. Transaction server **140** may include internal and external hardware components, as depicted and described in further detail with respect to FIG. **4**.

Authentication database **142** is a central storage for a set of user registered device data. Authentication database **142** can be implemented using any non-volatile storage medium known in the art. For example, authentication database can be implemented with a tape library, optical library, one or more independent hard disk drives, or multiple hard disk drives in a redundant array of independent disks (RAID). In this exemplary embodiment, authentication database **142** contains the computing device information for each registered user. For example, authentication database **142** may contain the serial number of a mobile cellular device and the name of the user who registered it.

FIG. **2** is a flowchart, **200**, depicting operational steps for setting up an online transaction verification program, in accordance with an embodiment of the present invention.

In step **202**, verification program **132** is installed on computing device **130**. In this exemplary embodiment, verification program **132** must be installed on computing device **130** prior to performing the transaction.

In step **204**, computing device **130** is registered with transaction server **140**. In this exemplary embodiment, this registration step allows transaction server **140** to associate the user with the specific computing device **130**.

In step **206**, transaction server **140** stores the registration data in authentication database **142**.

FIG. **3** is a flowchart, **300**, depicting operational steps for verifying online transaction integrity and authentication, in accordance with an embodiment of the present invention.

In step **302**, verification program **132** receives information associated with a QR code scan and displays the transaction details on computing device **130**. In this exemplary embodiment, computing device **120** receives a QR code containing encoded transaction details from transaction server **140**, via network **110** for the current online transaction being performed between computing device **120** and transaction server **140**. The online transaction is initiated by a user on computing device **120** that is received by transaction server **140**. Transaction server **140** generates a QR code and sends it back to computing device **120** for verification. It should be appreciated, that computing device **130** is preregistered with transaction server **140**, such that verification program **132** associates computing device **130** with a user. The QR code is scanned using computing device **130**, and verification program **132** decodes the transaction details. For example, a transaction may involve a user request to transfer money from a checking account to a savings account using computing device **120**. In this example, transaction server **140** is the bank server used to conduct online banking transactions. In this exemplary embodiment, the user can view the details of the online transaction between computing device **120** and transaction server **140** using computing device **130**.

In step **304**, verification program **132** prompts the user to determine whether the transaction details displayed on computing device **130** are consistent with the original transaction request. The transaction details displayed on computing device **130** are consistent with the original transaction when each object of the original transaction can be matched to a displayed transaction detail from the scanned and decoded QR code.

If, in step **304**, the user confirms the transaction details displayed on computing device **130** are consistent with the original transaction request, then in step **306**, verification program **132** sends a confirmation message to transaction server **140** using an out of band channel (i.e., the mobile device's data connection, SMS, initiate a call back, etc.). In this exemplary embodiment, as verification program **132** uses an alternate communication path to transmit confirmation, any possible MITM would be avoided during the confirmation step (step **304**). The MITM cannot access the out of band channel because the out of band channel is not directly associated with the access path to the application or data used in the online transaction. In addition, as computing device **130** is pre-registered with transaction server **140**, the confirmation message from verification program **132** provides an additional authentication. For example, when using computing device **120** to conduct an online banking transaction, transaction server **140** prompts the user for authentication (i.e., username and password). Thus, sending confirmation using computing device **130**, which is pre-registered with transaction server **140**, provides an additional authentication (in addition to username and password authentication). In this exemplary embodiment, transaction server **140** encrypts transaction details with its private key before generating the QR code and verification program **132** decrypts transaction details with transaction server **140** corresponding public key before displaying.

In step **308**, verification program **132** receives a response that the transaction has been completed from transaction server **140**. In this exemplary embodiment, transaction server **140** completes the original requested transaction when it receives the confirmation message from computing device **130** (step **306**).

If, in step **304**, the transaction details displayed on computing device **130** are not consistent with the original transaction request, then in step **310**, verification program **132** sends an abort message to transaction server **140** using an out of band channel responsive to the user selecting an abort button.

In step **312**, verification program **132** receives a response that the transaction has been aborted from transaction server **140**. In this exemplary embodiment, transaction server **140** aborts the original requested transaction when it receives the abort message from computing device **130** (step **310**).

Accordingly, by performing the operational steps of FIG. **2**, a secure transaction may be performed by a user, using an out-of-band channel to transmit a confirmation message for the transaction, thus avoiding a MITM. By preregistering a computing device with a transaction server, the confirmation message provides an additional authentication and ensures transactional integrity.

FIG. **4** is a block diagram of internal and external components of computing device **400**, which is representative of the computing devices of FIG. **1**, in accordance with an embodiment of the present invention. It should be appreciated that FIG. **4** provides only an illustration of one implementation and does not imply any limitations with regard to the environments in which different embodiments may be implemented. In general, the components illustrated in FIG. **4** are representative of any electronic device capable of executing machine-readable program instructions. Examples of computer systems, environments, and/or con-

figurations that may be represented by the components illustrated in FIG. **4** include, but are not limited to, personal computer systems, server computer systems, thin clients, thick clients, laptop computer systems, tablet computer systems, cellular telephones (i.e., smart phones), multiprocessor systems, microprocessor-based systems, network PCs, minicomputer systems, mainframe computer systems, and distributed cloud computing environments that include any of the above systems or devices.

Computing device **400** includes communications fabric **402**, which provides for communications between one or more processing units **404**, memory **406**, persistent storage **408**, communications unit **410**, and one or more input/output (I/O) interfaces **412**. Communications fabric **402** can be implemented with any architecture designed for passing data and/or control information between processors (such as microprocessors, communications and network processors, etc.), system memory, peripheral devices, and any other hardware components within a system. For example, communications fabric **402** can be implemented with one or more buses.

Memory **406** and persistent storage **408** are computer readable storage media. In this embodiment, memory **406** includes random access memory (RAM) **416** and cache memory **418**. In general, memory **406** can include any suitable volatile or non-volatile computer readable storage media. Software is stored in persistent storage **408** for execution and/or access by one or more of the respective processors **404** via one or more memories of memory **406**.

Persistent storage **408** may include, for example, a plurality of magnetic hard disk drives. Alternatively, or in addition to magnetic hard disk drives, persistent storage **408** can include one or more solid state hard drives, semiconductor storage devices, read-only memories (ROM), erasable programmable read-only memories (EPROM), flash memories, or any other computer readable storage media that is capable of storing program instructions or digital information.

The media used by persistent storage **408** can also be removable. For example, a removable hard drive can be used for persistent storage **408**. Other examples include optical and magnetic disks, thumb drives, and smart cards that are inserted into a drive for transfer onto another computer readable storage medium that is also part of persistent storage **408**.

Communications unit **410** provides for communications with other computer systems or devices via a network. In this exemplary embodiment, communications unit **410** includes network adapters or interfaces such as a TCP/IP adapter cards, wireless Wi-Fi interface cards, or 3G or 4G wireless interface cards or other wired or wireless communications links. The network can comprise, for example, copper wires, optical fibers, wireless transmission, routers, firewalls, switches, gateway computers and/or edge servers. Software and data used to practice embodiments of the present invention can be downloaded to computing device **400** through communications unit **410** (i.e., via the Internet, a local area network, or other wide area network). From communications unit **410**, the software and data can be loaded onto persistent storage **408**.

One or more I/O interfaces **412** allow for input and output of data with other devices that may be connected to computing device **400**. For example, I/O interface **412** can provide a connection to one or more external devices **420** such as a keyboard, computer mouse, touch screen, virtual keyboard, touch pad, pointing device, or other human interface devices. External devices **420** can also include portable computer readable storage media such as, for example, thumb drives, portable optical or magnetic disks, and memory cards. I/O interface **412** also connects to display **422**.

Display **422** provides a mechanism to display data to a user and can be, for example, a computer monitor. Display **422** can also be an incorporated display and may function as a touch screen, such as a built-in display of a tablet computer.

The present invention may be a system, a method, and/or a computer program product. The computer program product may include a computer readable storage medium (or media) having computer readable program instructions thereon for causing a processor to carry out aspects of the present invention.

The computer readable storage medium can be a tangible device that can retain and store instructions for use by an instruction execution device. The computer readable storage medium may be, for example, but is not limited to, an electronic storage device, a magnetic storage device, an optical storage device, an electromagnetic storage device, a semiconductor storage device, or any suitable combination of the foregoing. A non-exhaustive list of more specific examples of the computer readable storage medium includes the following: a portable computer diskette, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or Flash memory), a static random access memory (SRAM), a portable compact disc read-only memory (CD-ROM), a digital versatile disk (DVD), a memory stick, a floppy disk, a mechanically encoded device such as punch-cards or raised structures in a groove having instructions recorded thereon, and any suitable combination of the foregoing. A computer readable storage medium, as used herein, is not to be construed as being transitory signals per se, such as radio waves or other freely propagating electromagnetic waves, electromagnetic waves propagating through a waveguide or other transmission media (e.g., light pulses passing through a fiber-optic cable), or electrical signals transmitted through a wire.

Computer readable program instructions described herein can be downloaded to respective computing/processing devices from a computer readable storage medium or to an external computer or external storage device via a network, for example, the Internet, a local area network, a wide area network and/or a wireless network. The network may comprise copper transmission cables, optical transmission fibers, wireless transmission, routers, firewalls, switches, gateway computers and/or edge servers. A network adapter card or network interface in each computing/processing device receives computer readable program instructions from the network and forwards the computer readable program instructions for storage in a computer readable storage medium within the respective computing/processing device.

Computer readable program instructions for carrying out operations of the present invention may be assembler instructions, instruction-set-architecture (ISA) instructions, machine instructions, machine dependent instructions, microcode, firmware instructions, state-setting data, or either source code or object code written in any combination of one or more programming languages, including an object oriented programming language such as Smalltalk, C++ or the like, and conventional procedural programming languages, such as the "C" programming language or similar programming languages. The computer readable program instructions may execute entirely on the user's computer, partly on the user's computer, as a stand-alone software

package, partly on the user's computer and partly on a remote computer or entirely on the remote computer or server. In the latter scenario, the remote computer may be connected to the user's computer through any type of network, including a local area network (LAN) or a wide area network (WAN), or the connection may be made to an external computer (for example, through the Internet using an Internet Service Provider). In some embodiments, electronic circuitry including, for example, programmable logic circuitry, field-programmable gate arrays (FPGA), or programmable logic arrays (PLA) may execute the computer readable program instructions by utilizing state information of the computer readable program instructions to personalize the electronic circuitry, in order to perform aspects of the present invention.

Aspects of the present invention are described herein with reference to flowchart illustrations and/or block diagrams of methods, apparatus (systems), and computer program products according to embodiments of the invention. It will be understood that each block of the flowchart illustrations and/or block diagrams, and combinations of blocks in the flowchart illustrations and/or block diagrams, can be implemented by computer readable program instructions.

These computer readable program instructions may be provided to a processor of a general purpose computer, special purpose computer, or other programmable data processing apparatus to produce a machine, such that the instructions, which execute via the processor of the computer or other programmable data processing apparatus, create means for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks. These computer readable program instructions may also be stored in a computer readable storage medium that can direct a computer, a programmable data processing apparatus, and/or other devices to function in a particular manner, such that the computer readable storage medium having instructions stored therein comprises an article of manufacture including instructions which implement aspects of the function/act specified in the flowchart and/or block diagram block or blocks.

The computer readable program instructions may also be loaded onto a computer, other programmable data processing apparatus, or other device to cause a series of operational steps to be performed on the computer, other programmable apparatus or other device to produce a computer implemented process, such that the instructions which execute on the computer, other programmable apparatus, or other device implement the functions/acts specified in the flowchart and/or block diagram block or blocks.

The flowchart and block diagrams in the Figures illustrate the architecture, functionality, and operation of possible implementations of systems, methods, and computer program products according to various embodiments of the present invention. In this regard, each block in the flowchart or block diagrams may represent a module, segment, or portion of instructions, which comprises one or more executable instructions for implementing the specified logical function(s). In some alternative implementations, the functions noted in the block may occur out of the order noted in the figures. For example, two blocks shown in succession may, in fact, be executed substantially concurrently, or the blocks may sometimes be executed in the reverse order, depending upon the functionality involved. It will also be noted that each block of the block diagrams and/or flowchart illustration, and combinations of blocks in the block diagrams and/or flowchart illustration, can be implemented by special purpose hardware-based systems that perform the specified functions or acts or carry out combinations of special purpose hardware and computer instructions.

The descriptions of the various embodiments of the present invention have been presented for purposes of illustration, but are not intended to be exhaustive or limited to the embodiments disclosed. Many modifications and variations will be apparent to those of ordinary skill in the art without departing from the scope and spirit of the invention. The terminology used herein was chosen to best explain the principles of the embodiment, the practical application or technical improvement over technologies found in the marketplace, or to enable others of ordinary skill in the art to understand the embodiments disclosed herein.

What is claimed is:

1. A computer-implemented method for verifying transactions over a network comprising:

providing, by a first computing device details of a proposed transaction to a transaction server;

receiving, by said first computing device a QR code, wherein the QR code comprises encoded details of the proposed transaction, in response to said providing, by a first computing device details of a proposed transaction to a transaction server;

scanning, by said first computing device, the QR code;

decoding, by an application of said first computing device, the QR code;

comparing, by one or more computer processors, a set of transaction details associated with the decoded QR code to the details of the proposed transaction; and

confirming, by a separate communication channel, the proposed transaction, wherein the separate communication channel is out of band to an access path to the application.

2. The method of claim **1**, wherein said proposed transaction is conducted between a second computing device and said transaction server.

3. The method of claim **1**, further comprising:

registering, by one or more computer processors, the first computing device with said transaction server.

4. The method of claim **1**, wherein said QR code contains information associated with said transaction.

5. The method of claim **1**, wherein confirming the proposed transaction occurs between the first computing device and said transaction server.

6. The method of claim **1**, wherein confirming the proposed transaction comprises:

prompting, by one or more computer processors, a determination of whether said set of transaction details associated with the QR code matches the details of the proposed transaction; and

responsive to receiving an indication that said set of transaction details associated with the QR code matches the details of the proposed transaction, sending, by one or more computer processors, a confirm message to said transaction server confirming said proposed transaction.

7. The method of claim **1**, further comprising:

prompting, by one or more computer processors, a determination of whether said set of transaction details associated with the QR code matches the details of the proposed transaction; and

responsive to receiving an indication that said set of transaction details associated with the QR code does not match the details of the proposed transaction,

sending, by one or more computer processors, an abort message to said transaction server cancelling said proposed transaction.

8. A computer program product comprising:

a computer readable storage medium and program instructions stored on the computer readable storage medium, the program instructions comprising:

program instructions to provide details of a proposed transaction to a transaction server;

program instructions to receive, a QR code, wherein the QR code comprises encoded details of the proposed transaction, in response to said program instructions to provide details of a proposed transaction to a transaction server;

program instructions to scan the QR code by a first computing device;

program instructions to decode the QR code using an application of said first computing device;

program instructions to compare a set of transaction details associated with the decoded QR code to the details of the proposed transaction; and

program instructions to confirm the proposed transaction by a separate communication channel, wherein the separate communication channel is out of band to an access path to the application used in the transaction.

9. The computer program product of claim **8**, wherein said proposed transaction is conducted between a second computing device and said transaction server.

10. The computer program product of claim **8**, further comprising:

program instructions to register the first computing device with said transaction server.

11. The computer program product of claim **8**, wherein said QR code contains information associated with said transaction.

12. The computer program product of claim **8**, wherein the program instructions to confirm the proposed transaction occurs between the first computing device and said transaction server.

13. The computer program product of claim **8**, wherein the program instructions to confirm the proposed transaction comprise:

program instructions to prompt a determination of whether said set of transaction details associated with the QR code matches the details of the proposed transaction; and

program instructions to, responsive to receiving an indication that said set of transaction details associated with the QR code matches the details of the proposed transaction, send a confirm message to said transaction server confirming said proposed transaction.

14. The computer program product of claim **8**, further comprising:

program instructions to prompt a determination of whether said set of transaction details associated with the QR code matches the details of the proposed transaction; and

program instructions to, responsive to receiving an indication that said set of transaction details associated with the QR code does not match the details of the proposed transaction, send an abort message to said transaction server cancelling said proposed transaction.

15. A computer system comprising:

one or more computer processors;

one or more computer readable storage media;

program instructions stored on the computer readable storage media for execution by at least one of the one or more computer processors, the program instructions comprising:

program instructions to provide details of a proposed transaction to a transaction server;

program instructions to receive a QR code, wherein the QR code comprises encoded details of the proposed transaction, in response to said program instructions to provide details of a proposed transaction to a transaction server;

program instructions to scan the QR code by a first computing device;

program instructions to decode the QR code using an application of said first computing device;

program instructions to compare a set of transaction details associated with the decoded QR code to the details of the proposed transaction; and

program instructions to confirm the proposed transaction by a separate communication channel, wherein the separate communication channel is out of band to the application used in the transaction.

16. The computer system of claim **15**, wherein said proposed transaction is conducted between a second computing device and said transaction server.

17. The computer system of claim **15**, further comprising:

program instructions to register the first computing device with said transaction server.

18. The computer system of claim **15**, wherein the program instructions to confirm the proposed transaction occurs between the first computing device and said transaction server.

19. The computer system of claim **15**, wherein the program instructions to confirm the proposed transaction comprise:

program instructions to prompt a determination of whether said set of transaction details associated with the QR code matches the details of the proposed transaction; and

program instructions to, responsive to receiving an indication that said set of transaction details associated with the QR code matches the details of the proposed transaction, send a confirm message to said transaction server confirming said proposed transaction.

20. The computer system of claim **15**, further comprising:

program instructions to prompt a determination of whether said set of transaction details associated with the QR code matches the details of the proposed transaction; and

program instructions to, responsive to receiving an indication that said set of transaction details associated with the QR code does not match the details of the proposed transaction, send an abort message to said transaction server cancelling said proposed transaction.

* * * * *

9.7 Detecting and Defending Against Man-in-the-Middle Attacks


US008533821B2

(12) **United States Patent**
Crume

(10) **Patent No.: US 8,533,821 B2**
(45) **Date of Patent: Sep. 10, 2013**

(54) **DETECTING AND DEFENDING AGAINST MAN-IN-THE-MIDDLE ATTACKS**

(75) Inventor: **Jeffery L. Crume**, Raleigh, NC (US)

(73) Assignee: **International Business Machines Corporation**, Armonk, NY (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 1083 days.

(21) Appl. No.: **11/753,673**

(22) Filed: **May 25, 2007**

(65) **Prior Publication Data**

US 2008/0295169 A1 Nov. 27, 2008

(51) **Int. Cl.**
G06F 11/00 (2006.01)

(52) **U.S. Cl.**
USPC **726/22**; 726/23; 726/24; 726/25; 726/30; 713/165; 713/169

(58) **Field of Classification Search**
USPC 726/22–26; 713/165, 172, 181, 713/182
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,310,720	A	1/1982	Check, Jr.
5,046,082	A	9/1991	Zicker et al.
5,068,894	A	11/1991	Hoppe
5,323,465	A	6/1994	Avarne
5,457,737	A	10/1995	Wen
5,491,752	A	2/1996	Kaufman et al.
5,497,411	A	3/1996	Pellerin
5,647,388	A	7/1997	Butler, Jr. et al.
5,657,388	A	8/1997	Weiss
5,684,950	A	11/1997	Dare et al.
5,701,339	A	12/1997	Suda
5,749,052	A	5/1998	Hidem et al.
5,841,871	A	11/1998	Pinkas
5,842,124	A	11/1998	Kenagy et al.
5,892,902	A	4/1999	Clark
5,953,422	A	9/1999	Angelo et al.
5,971,272	A	10/1999	Hsiao
6,000,031	A	12/1999	Bingaman et al.
6,169,890	B1	1/2001	Vatanen
6,278,863	B1	8/2001	Mabrouki
6,308,268	B1	10/2001	Audebert

(Continued)

FOREIGN PATENT DOCUMENTS

DE	10317176	11/2004
DE	103171176 A1	11/2004

(Continued)

OTHER PUBLICATIONS

Geneiatakis D, Survey of Security vulnerabilities in session initiation protocol, Aug. 2006, IEEE, vol. 8, Issue 3, pp. 7-10.*

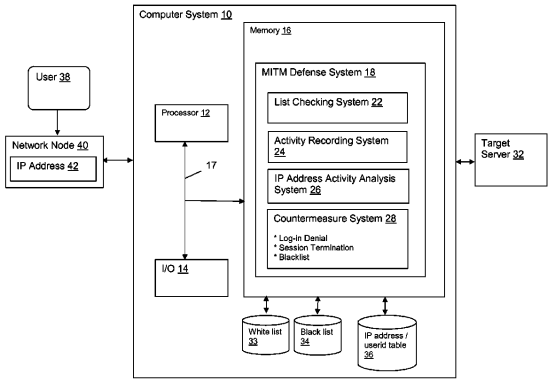
(Continued)

Primary Examiner — Nathan Flynn
Assistant Examiner — Viral Lakhia
(74) *Attorney, Agent, or Firm* — Douglas A. Lashmit; Hoffman Warnick LLC

(57) **ABSTRACT**

A system, method and program product for defending against man in the middle (MITM) attacks directed at a target server. A system is provided that includes an activity recording system that records an incoming IP address, userid, and time of each session occurring with the target server; an activity analysis system that identifies suspect IP addresses by determining if an unacceptable number of sessions are occurring from a single incoming IP address during a predefined time period; and a countermeasure system for taking action against suspect IP addresses.

13 Claims, 4 Drawing Sheets



(56) **References Cited**

U.S. PATENT DOCUMENTS

6,324,271 B1 11/2001 Sawyer et al.
6,330,608 B1 12/2001 Stiles
6,334,056 B1 12/2001 Holmes et al.
6,338,140 B1 1/2002 Owens et al.
6,349,134 B1 2/2002 Katz
6,385,729 B1 5/2002 DiGiorgio et al.
6,387,729 B2 5/2002 Eng et al.
6,393,468 B1 5/2002 McGee
6,400,726 B1 6/2002 Piret et al.
6,466,780 B1 10/2002 Geiselman et al.
6,535,726 B1 3/2003 Johnson
6,584,309 B1 6/2003 Whigham
6,687,241 B1 2/2004 Goss
6,707,915 B1 3/2004 Jobst et al.
6,731,731 B1 5/2004 Ueshima
6,993,658 B1 1/2006 Engberg et al.
6,993,663 B1 1/2006 Paya et al.
7,007,301 B2 2/2006 Crosbie et al.
7,024,688 B1 4/2006 Faccin et al.
7,028,179 B2 * 4/2006 Anderson et al. 713/154
7,058,796 B2 6/2006 Lynn et al.
7,058,968 B2 * 6/2006 Rowland et al. 726/1
7,100,204 B1 8/2006 Myllymaki et al.
7,133,662 B2 11/2006 Bravo et al.
7,142,840 B1 11/2006 Geddes et al.
7,221,949 B2 5/2007 Clough
7,290,278 B2 10/2007 Cahill et al.
7,317,693 B1 * 1/2008 Roesch et al. 370/252
7,324,976 B2 1/2008 Gupta et al.
7,337,431 B1 2/2008 Barnes et al.
7,357,310 B2 4/2008 Calabrese et al.
7,360,248 B1 4/2008 Kanevsky et al.
7,376,431 B2 5/2008 Niedermeyer
7,379,921 B1 5/2008 Kiliccote
7,380,708 B1 6/2008 Kiliccote
7,447,494 B2 11/2008 Law et al.
7,480,805 B1 * 1/2009 Gnech et al. 713/183
7,491,308 B2 * 2/2009 Talieh et al. 205/137
7,519,989 B2 4/2009 Lin et al.
7,533,414 B1 * 5/2009 Reed et al. 726/22
7,536,634 B2 * 5/2009 Green et al. 715/200
7,540,022 B2 5/2009 Barari et al.
7,594,270 B2 * 9/2009 Church et al. 726/23
7,600,676 B1 10/2009 Rados et al.
7,609,625 B2 * 10/2009 Wei et al. 370/229
7,623,458 B2 * 11/2009 Ayyagari et al. 370/235
7,624,447 B1 * 11/2009 Horowitz et al. 726/23
7,665,128 B2 * 2/2010 Yang 726/11
7,673,334 B2 * 3/2010 Takemori et al. 726/10
7,715,823 B2 5/2010 Bravo et al.
7,716,742 B1 * 5/2010 Roesch et al. 726/25
7,757,285 B2 * 7/2010 Kubota 726/23
7,765,584 B2 7/2010 Roskind
7,779,465 B2 * 8/2010 Baker et al. 726/22
7,823,199 B1 * 10/2010 Rathi et al. 726/22
7,840,993 B2 11/2010 Ganesan et al.
7,845,004 B2 * 11/2010 Bardsley et al. 726/22
7,886,346 B2 2/2011 Sandhu et al.
7,926,108 B2 * 4/2011 Rand et al. 726/22
7,930,540 B2 4/2011 Ahuja et al.
7,954,150 B2 * 5/2011 Croft et al. 726/21
7,975,293 B2 7/2011 Yoshida et al.
8,019,995 B2 9/2011 van Bemmel
8,024,567 B2 9/2011 Han
8,050,658 B2 11/2011 Hong
8,060,915 B2 11/2011 Voice et al.
8,117,449 B2 2/2012 Blythe
8,136,150 B2 3/2012 Hayler et al.
8,150,370 B2 4/2012 Dempo et al.
8,151,327 B2 * 4/2012 Eisen 726/5
8,181,248 B2 * 5/2012 Oh et al. 726/23
8,201,217 B1 6/2012 Begen et al.
8,254,542 B2 8/2012 Frederick
8,281,375 B2 10/2012 von Krogh
8,285,639 B2 10/2012 Eden et al.
8,296,823 B2 10/2012 Schubert
8,301,877 B2 10/2012 Grajek et al.
8,302,180 B1 10/2012 Gudov et al.
8,302,187 B1 10/2012 Gupta et al.
2001/0054155 A1 * 12/2001 Hagan et al. 713/193
2002/0069165 A1 6/2002 O'Neil
2002/0091931 A1 7/2002 Quick et al.
2002/0095588 A1 7/2002 Shigematsu et al.
2002/0178070 A1 11/2002 Leveridge
2002/0178370 A1 11/2002 Gurevich et al.
2003/0014315 A1 1/2003 Jaalinoja et al.
2003/0154382 A1 8/2003 Vicard
2003/0172272 A1 9/2003 Ehlers et al.
2004/0148520 A1 7/2004 Talpade et al.
2004/0152446 A1 8/2004 Saunders et al.
2004/0198329 A1 10/2004 Vasa
2005/0015624 A1 1/2005 Ginter et al.
2005/0018618 A1 * 1/2005 Mualem et al. 370/252
2005/0022020 A1 1/2005 Fremberg
2005/0060535 A1 * 3/2005 Bartas 713/154
2005/0075070 A1 4/2005 Crilly, Jr.
2005/0182958 A1 * 8/2005 Pham et al. 713/200
2005/0187934 A1 * 8/2005 Motsinger et al. 707/9
2005/0188423 A1 * 8/2005 Motsinger et al. 726/22
2005/0210251 A1 9/2005 Nyberg et al.
2006/0021031 A1 * 1/2006 Leahy et al. 726/22
2006/0036690 A1 * 2/2006 O'Neil 709/206
2006/0094403 A1 5/2006 Norefors et al.
2006/0095955 A1 5/2006 Vong et al.
2006/0288411 A1 12/2006 Garg et al.
2007/0015492 A1 1/2007 Bravo et al.
2007/0067828 A1 3/2007 Bychkov
2007/0083606 A1 * 4/2007 Malik et al. 709/207
2007/0084913 A1 4/2007 Weston
2007/0107050 A1 5/2007 Selvarajan
2007/0136573 A1 6/2007 Steinberg
2007/0136808 A1 * 6/2007 Xiong 726/22
2007/0143851 A1 * 6/2007 Nicodemus et al. 726/25
2007/0186099 A1 8/2007 Beck et al.
2007/0234426 A1 10/2007 Khanolkar et al.
2007/0261112 A1 11/2007 Todd et al.
2007/0266257 A1 11/2007 Camaisa et al.
2008/0028447 A1 1/2008 O'Malley et al.
2008/0172730 A1 7/2008 Sandhu et al.
2008/0181380 A1 7/2008 Gustave et al.
2008/0189776 A1 8/2008 Constable
2008/0209275 A1 8/2008 Kwan et al.
2008/0270301 A1 10/2008 Jones et al.
2008/0281737 A1 11/2008 Fajardo
2008/0318548 A1 12/2008 Bravo et al.
2009/0037329 A1 2/2009 Coppinger et al.
2009/0077637 A1 3/2009 Santos et al.
2009/0094682 A1 4/2009 Sage et al.
2009/0095588 A1 4/2009 Thomas
2009/0104889 A1 4/2009 Lotvonen et al.
2009/0106138 A1 4/2009 Smith et al.
2009/0300738 A1 12/2009 Dewe et al.
2010/0024017 A1 1/2010 Ashfield et al.
2010/0051686 A1 3/2010 Obi
2010/0095351 A1 4/2010 Liu et al.
2010/0269162 A1 10/2010 Bravo et al.
2011/0015449 A1 1/2011 Pendleton et al.
2011/0039237 A1 2/2011 Skare
2011/0138483 A1 6/2011 Bravo et al.
2011/0197070 A1 8/2011 Mizrah
2011/0225647 A1 9/2011 Dilley et al.
2011/0277024 A1 11/2011 Begley et al.
2011/0289576 A1 11/2011 Cheng
2012/0011066 A1 1/2012 Telle et al.
2012/0149334 A1 6/2012 Zhang et al.
2012/0204241 A1 8/2012 Varsavsky et al.
2012/0264405 A1 10/2012 Bravo et al.
2012/0272331 A1 10/2012 Lemaster et al.

FOREIGN PATENT DOCUMENTS

EP 1119147 A1 7/2001
GB 2456509 A 7/2009
JP 10334048 12/1998
JP 10341224 12/1998

JP	2001111545		4/2001
WO	0109808	A1	8/2001
WO	2004079499	A2	9/2004
WO	2006103387	A1	10/2006
WO	2008147353	A1	12/2008

OTHER PUBLICATIONS

Juels, A., "Strengthening EPC Tags Against Cloning." WiSE '05, Sep. 2, 2005. pp. 67-75.

Lee, S. & Choi, Y., "A Resilient Packet-Forwarding Scheme against Maliciously Packet-Dripping Nodes in Sensor Networks." SASN '06, Oct. 30, 2006. pp. 59-69.

Deng, R., Zhou, J., & Bao, F., "Defending Against Redirect Attacks in Mobile IP." CCS '02, Nov. 18-22, 2002. pp. 59-67.

Kaafar, M., Mathy, L., Turletti, T., & Dabbous, W., "Real attacks on virtual networks: Vivaldi out of tune." SIGCOMM '06 Workshops, Sep. 11-15, 2006. pp. 139-146.

Lakhia, U.S. Appl. No. 13/432,956, Office Action 1, IBMC-0208-CON, Feb. 14, 2013, 26 pages.

Gee, U.S. Appl. No. 13/084,823, Office Action, IBMC-0395, Mar. 11, 2013, 8 pages.

Leung, "Depress Phishing by CAPTCHA with OTP", Department of Information Engineering The Chinese University of Hong Kong, IEEE 2009, 6 pgs.

Kopsidas et al., "Voice Interactive Personalized Security (VoIPSEC) protocol: Fortify Internet telephony by providing end-to-end security through inbound key exchange and biometric verification", 2006 IEEE, 10 pgs.

Koo et al., "VoIP Interception in P2P SIP Environment", 2010 IEEEE, vol. 1, pp. 331-334.

Megeed, U.S. Appl. No. 12/423,928, Office Action 1, IBMC-0326, 21 pages, Aug. 25, 2011.

Megeed, U.S. Appl. No. 12/423,928, Final Office Action 1, IBMC-0326, 20 pages, Nov. 10, 2011.

Megeed, U.S. Appl. No. 12/423,928, Office Action 2, IBMC-0326, 20 pages, Jun. 8, 2012.

Megeed, U.S. Appl. No. 12/423,928, Notice of Allowance 1, IBMC-0326, 10 pages, Sep. 25, 2012.

Megeed, U.S. Appl. No. 12/423,928, Notice of Allowance 2, IBMC-0326, 19 pages, Dec. 4, 2012.

Bibbee, U.S. Appl. No. 11/765,193, Office Action 1, 15 pages, Feb. 18, 2010.

Bibbee, U.S. Appl. No. 11/765,193, Office Action 2, 14 pages, Nov. 29, 2010.

Bibbee, U.S. Appl. No. 11/765,193, Office Action 3, 18 pages, Sep. 19, 2011.

Bibbee, U.S. Appl. No. 11/765,193, Final Office Action 1, 15 pages, Jul. 30, 2010.

Bibbee, U.S. Appl. No. 11/765,193, Final Office Action 2, 17 pages, May 12, 2011.

Bibbee, U.S. Appl. No. 11/765,193, Final Office Action 3, 18 pages, Apr. 16, 2012.

Tran, U.S. Appl. No. 11/524,340, Office Action, 9 pages, Jul. 29, 2009.

Tran, U.S. Appl. No. 11/524,340, Office Action, 19 pages, Oct. 31, 2008.

Tran, U.S. Appl. No. 11/524,340, Notice of Allowance, 11 pages, Dec. 29, 2009.

Tran, U.S. Appl. No. 11/524,340, Office Action, 7 pages, Apr. 29, 2009.

Tran, U.S. Appl. No. 11/524,340, Office Action, 22 pages, May 27, 2008.

Alicherry et al., "DoubleCheck: Multi-ath Verification Against Man-in-the-Middle Attack", IEEE 2009, pp. 557-563.

Kumaraguru et al., "Getting Users to Pay Attention to Anti-Phishing Education: Evaluation of Retention and Transfer", APWG eCrime Researchers Summit, Oct. 4-5, 2007, Pittsburgh, PA pp. 70-81.

Adida, "BeamAuth: Two-Factor Web Authentication with a Bookmark", CCS '07, Oct. 29-Nov. 2, 2007, Alexandria, VA, ACM 978-1-59593-703-2107/0010, pp. 48-57.

Nassar et al., "Holistic VoIP Intrusion Detection and Prevention System", IPTCOMM '07, ACM 2007, pp. 1-9.

Stoll et al., "Sesame: Informing User Security Decisions with System Visualization", CHI 2008 Proceedings, Am I Safe, Apr. 5-10, 2008, Florence, Italy, pp. 1045-1054.

Bonzo, U.S. Appl. No. 11/776,619, Notice of Allowance, Apr. 29, 2010, 10 pages.

Bonzo, U.S. Appl. No. 11/776,619, Office Action, Sep. 30, 2009, 12 pages.

"Prevent Online Banking Fraud", Dec. 7, 2010, http://www.phonefactor.com/products/transaction-verification, 1 pages.

Geneiatakis et al., "Survey of Security Vulnerabilities in Session Initiation Protocol", 3rd Quarter 2006, vol. 8, No. 3, IEEE Communications Surveys & Tutorials, pp. 68-81.

Almeida, U.S. Appl. No. 12/630,875, Office Action, IBMC-0353, Mar. 1, 2012, 17 pages.

Almeida, U.S. Appl. No. 12/630,875, Office Action, IBMC-0353, Aug. 30, 2012, 14 pages.

Almeida, U.S. Appl. No. 12/630,875, Notice of Allowance, IBMC-0353, Dec. 20, 2012, 7 pages.

Bibbee, U.S. Appl. No. 11/765,193, Examiner's Answer, Apr. 16, 2013, 20 pages.

Almeida, U.S. Appl. No. 12/630,875, Office Action, Apr. 17, 2013, 40 pages.

Ma et al., "Beyond Blacklists: Learning to Detect Malicious Web Sites from Suspicious URLs", KDD'09, Jul. 28-Jul. 1, 2009, pp. 1245-1253.

Lakhia, U.S. Appl. No. 13/432,956, Notice of Allowance & Fees Due, Apr. 15, 2013, 27 pages.

* cited by examiner

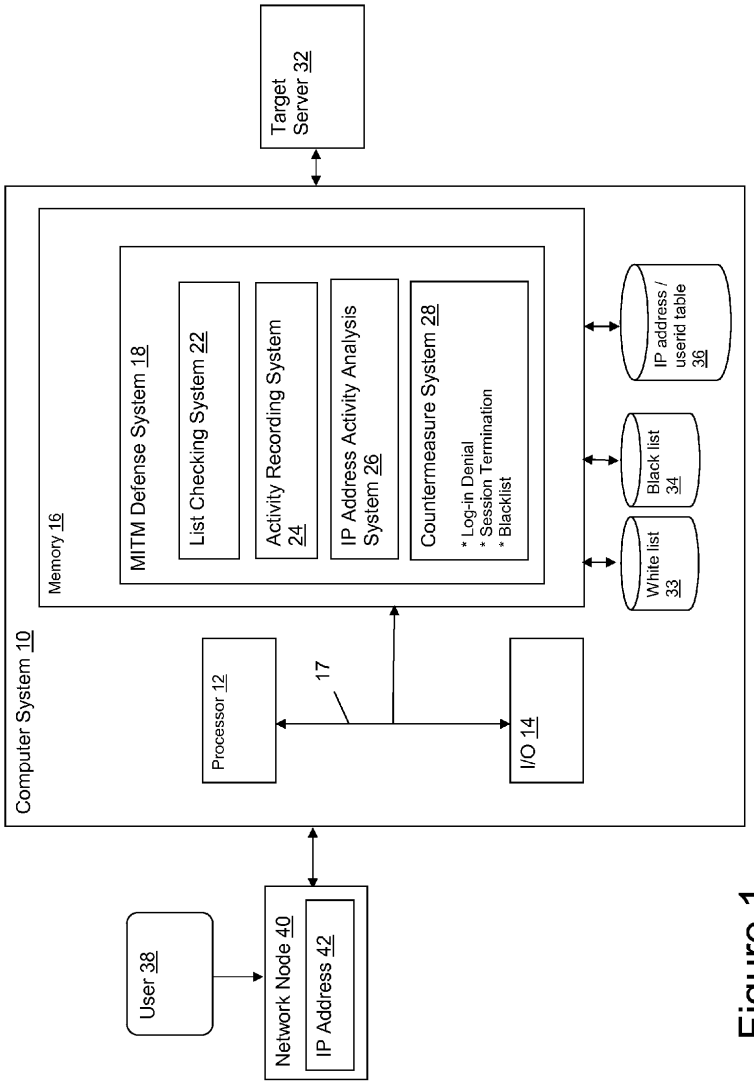

Target Server 32
Computer System 10
Memory 16
MITM Defense System 18
List Checking System 22
Activity Recording System 24
IP Address Activity Analysis System 26
Countermeasure System 28
* Log-in Denial
* Session Termination
* Blacklist
IP address / userid table 36
Black list 34
White list 33
Processor 12
17
I/O 14
User 38
Network Node 40
IP Address 42

Figure 1

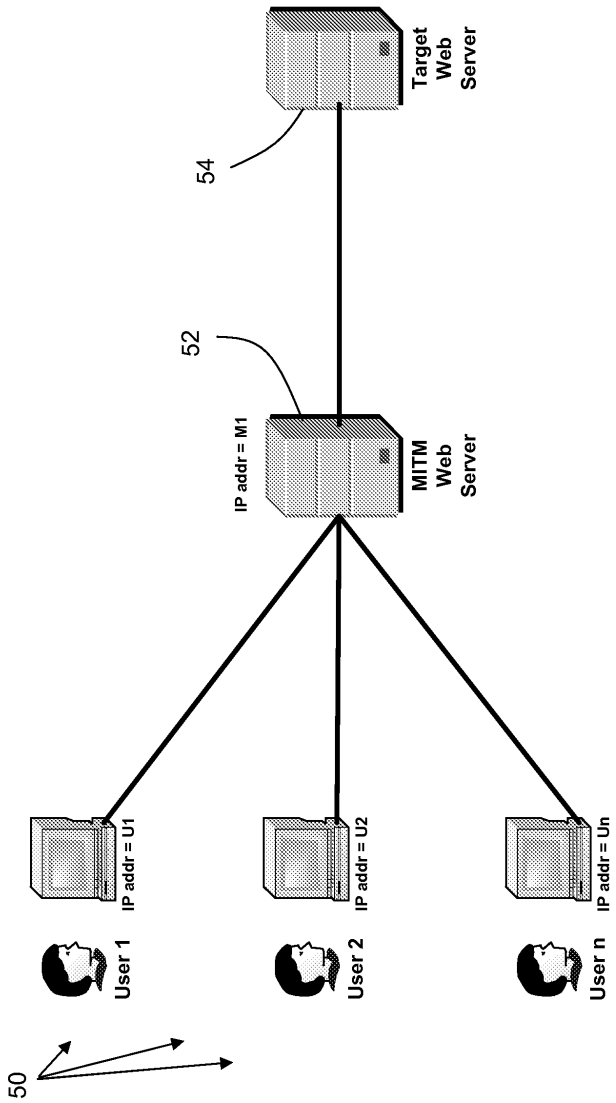

Target Web Server
54
52
IP addr = M1
MITM Web Server
IP addr = U1
IP addr = U2
IP addr = Un
User 1
User 2
User n
50

Figure 2

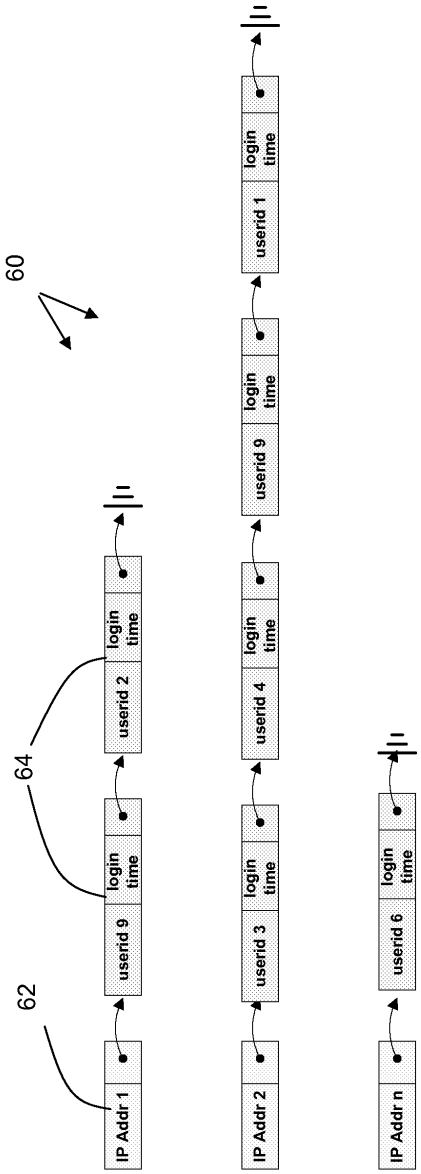

60
62
64
IP Addr 1
userid 9
login time
userid 2
login time
IP Addr 2
userid 3
login time
userid 4
login time
userid 9
login time
userid 1
login time
IP Addr n
userid 6
login time

Figure 3

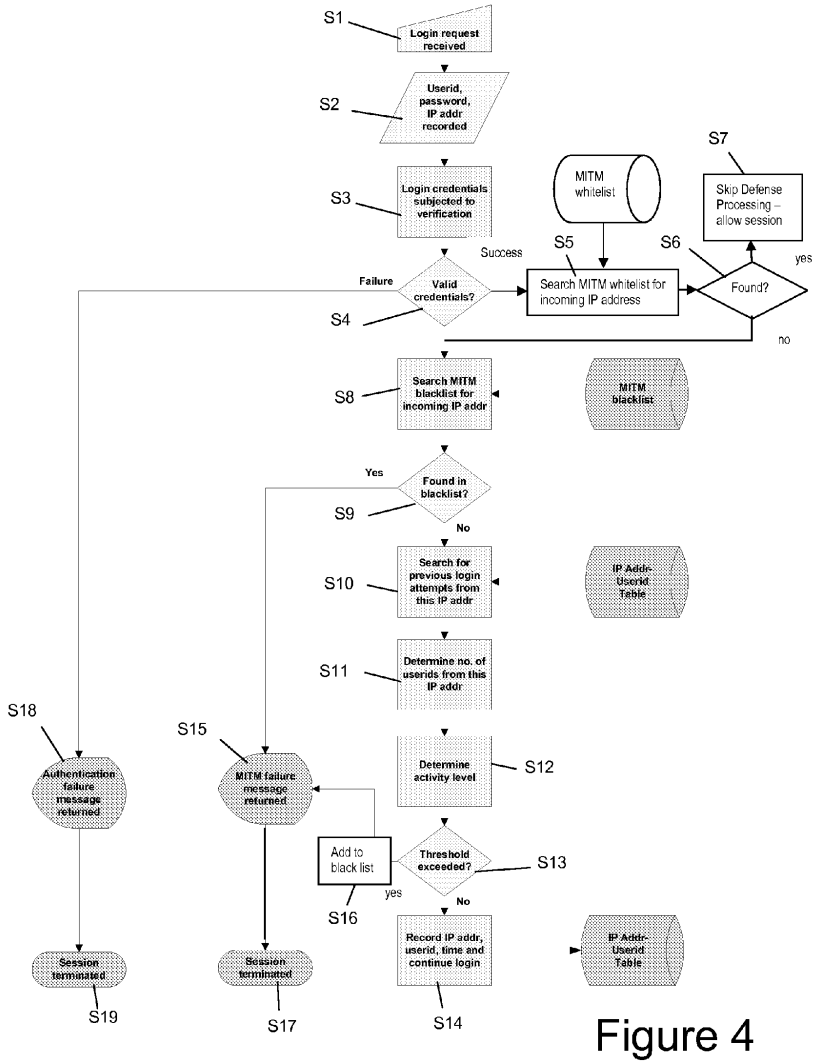

S1
Login request received
S2
Userid, password, IP addr recorded
S3
Login credentials subjected to verification
Success
Failure
Valid credentials?
S4
MITM whitelist
S5
Search MITM whitelist for incoming IP address
S6
Found?
yes
no
S7
Skip Defense Processing – allow session
S8
Search MITM blacklist for incoming IP addr
MITM blacklist
Yes
Found in blacklist?
S9
No
S10
Search for previous login attempts from this IP addr
IP Addr-Userid Table
S11
Determine no. of userids from this IP addr
S12
Determine activity level
Threshold exceeded?
S13
Add to black list
yes
S16
No
Record IP addr, userid, time and continue login
IP Addr-Userid Table
S14
S15
MITM failure message returned
Session terminated
S17
S18
Authentication failure message returned
Session terminated
S19

Figure 4

DETECTING AND DEFENDING AGAINST MAN-IN-THE-MIDDLE ATTACKS

FIELD OF THE INVENTION

This disclosure relates generally to protecting the integrity of network communications, and more particularly to a system and method of detecting and defending against man-in-the-middle (MITM) attacks.

BACKGROUND OF THE INVENTION

One of the most difficult network-based attacks to defend against is that of a class known as "man-in-the-middle" (MITM) attacks. These scenarios involve the insertion by an attacker of an untrusted node into a session path. This MITM attack node then impersonates the identity of one session partner to the other while having access to and control over all transmissions between the partners resulting in the potential for eavesdropping and unauthorized modification of session traffic. These attacks are particularly effective when combined with "phishing" techniques which trick an end user into giving up personal information that later results in identity theft or fraud.

FIG. **2** depicts an example of an MITM attack, in which a plurality of users **50** are unsuspectingly engaged in sessions with an MITM Web server **52**, which sits between users **50** and the legitimate target Web server **54**. In this case, MITM Web server **52** has lured users **50** into believing that they are engaging in a session with the target Web server **54**.

Banks and other financial institutions have been particularly hard hit by these attacks as customers are lured into logging onto a malicious MITM node thinking they are connecting to their bank, while the MITM node interacts with the legitimate web site and relays information to the user making the ruse even more believable. It is this last aspect that is particularly distressing to banks as they do not have a good way to detect that they are dealing with an MITM node rather than directly with their customer. Because the attacker's MITM machine looks and acts just like a real end user, the MITM machine acts as a conduit for sensitive information such as userids and passwords and, potentially, for conducting transactions.

While digital certificates could provide a reasonable measure of protection in such an instance, they have thus far proven to be difficult and expensive to deploy and manage across a large end user base especially when those users may have limited technical skills and may also be highly mobile, using many different nodes to conduct transactions.

Another increasingly popular defense is to use "strong" authentication mechanisms such as security tokens, smart cards or biometrics to ensure that the end user is who they claim to be. The problem with these defenses is that in the MITM case, the digitized authentication data is simply passed directly through the intermediate node making it unnecessary for the attacker to actually possess the token, smart card or physical characteristic being measured.

Finally, another technique for alerting end users that they are being lured into logging into a bogus Web site involves the presentation of a graphical image pre-selected by the user. During login, if the user does not see the image they selected during registration (something which only they and the legitimate Web site should know), then they know to abort the authentication process. However, in an MITM case, the target Web site presents the image to the MITM node thinking it is the end user and the MITM node relays this image to the real end user leading them to believe that the attack node is legitimate.

SUMMARY OF THE INVENTION

The present invention relates to a system, method and program product for detecting man in the middle attacks. In one embodiment, there is a system for defending against man in the middle (MITM) attacks directed at a target server, comprising: an activity recording system that records an incoming IP address, userid, and time of each session occurring with the target server; an activity analysis system that identifies suspect IP addresses by determining if an unacceptable number of sessions are occurring from a single incoming IP address during a predefined time period; and a countermeasure system for taking action against suspect IP addresses.

In a second embodiment, there is a computer program product stored on a computer readable medium, which when executed includes program instructions for defending against man in the middle (MITM) attacks directed at a target server, the program product comprising: program instructions for recording an incoming IP address, userid, and time of each session occurring with the target server; program instructions for identifying suspect IP addresses by determining if an unacceptable number of sessions are occurring from a single incoming IP address during a predefined time period; and program instructions for taking defensive action against suspect IP addresses.

In a third embodiment, there is method for defending against man in the middle (MITM) attacks directed at a target server, comprising: recording an incoming IP address, userid, and time of each session occurring with the target server; identifying suspect IP addresses by determining if an unacceptable number of sessions are occurring from a single incoming IP address during a predefined time period; and taking defensive action against suspect IP addresses.

In a fourth embodiment, there is a method for deploying a system for defending against man in the middle (MITM) attacks directed at a target server, comprising: providing a computer infrastructure being operable to: record an incoming IP address, userid, and time of each session occurring with the target server; identify suspect IP addresses by determining if an unacceptable number of sessions are occurring from a single incoming IP address during a predefined time period; and take defensive action against suspect IP addresses.

MITM attacks of the sort described herein share a detectable characteristic that can be used to predict to some reasonable certainty that an attack is taking place. Once detected, defensive action can be taken, such as sending a message that will be relayed by the MITM node to the user informing the user of the potential vulnerability and ending the session.

The observable characteristic shared by successful MITM attacks is that to the target server it will appear that a large number of different end users have for no apparent reason begun logging on from the same IP address, i.e., the address of the MITM proxy. If, for instance, certain definable thresholds were exceeded such as N number of userids from a single, previously unknown address within a specific interval of time, then further investigation or even automated defenses would be warranted.

Some advantages to this technique include: the thresholds can be tuned to suit the risk tolerance of the target organization; detection can be automated; countermeasures can be automated to limit further damage; automated detection and response allows for constant vigilance by providing a con-

tinuous, 24×7 defense; the basic technique can be extended beyond web spoofing/phishing attacks to other types of MITM scenarios; the more "successful" the attacker is at luring victims, the more likely the attack will be detected and repelled

The illustrative aspects of the present invention are designed to solve the problems herein described and other problems not discussed.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other features of this invention will be more readily understood from the following detailed description of the various aspects of the invention taken in conjunction with the accompanying drawings.

FIG. **1** depicts a computer system having an MITM defense system in accordance with an embodiment of the present invention.

FIG. **2** depicts an example of an MITM attack.

FIG. **3** depicts an example of a IP address/userid table in accordance with an embodiment of the present invention.

FIG. **4** depicts a flow diagram showing an illustrative implementation of an embodiment of the present invention.

The drawings are merely schematic representations, not intended to portray specific parameters of the invention. The drawings are intended to depict only typical embodiments of the invention, and therefore should not be considered as limiting the scope of the invention. In the drawings, like numbering represents like elements.

DETAILED DESCRIPTION OF THE INVENTION

FIG. **1** depicts a computer system **10** that provides an MITM defense system **18** for a target server **32** communicating with a user **38** via network node **40**. In particular, MITM defense system **18** analyzes the IP address **42** of network node **40** to determine whether network node **40** is a legitimate node associated with user **38** or an MITM server that has interposed itself between the user **38** and target server **32**. Note that in this illustrative embodiment, computer system **10** containing MITM defense system **18** is shown separated from target server **32**. However, it is understood that MITM defense system **18** may be integrated with target server **32** in a single system.

As noted above, an observable characteristic shared by successful MITM attacks is that it will appear to the target server **32** that a large number of different end users have for no apparent reason begun logging on from the same IP address **42**, i.e., the address of the MITM server. While this behavior alone will not conclusively indicate malicious activity, identifying and analyzing such behavior can allow for further investigation or countermeasures to be taken. For instance, definable thresholds involving the allowed number of user IDs from a single, previously unknown address within a specific interval of time can be put in place to identify suspicious activity. When a threshold is exceeded, then further investigation or even automated defenses can be implemented.

As shown in this illustrative embodiment, MITM defense system **18** includes a list checking system **22**, an activity recording system **24**, an IP address activity analysis system **26**, and a countermeasure system **28**. List checking system **22** is utilized to compare an incoming IP address **42** with either or both a white list **33** and a black list **34**. The white list **33** may include a list of known IP addresses that are valid, and need not be analyzed (e.g., the IP address associated with a known legitimate proxy, etc.). The black list **34** may include a list of known IP addresses that are invalid (e.g., sites that are known to have caused attacks in the past). When an IP address **42** is found on the black list **34**, the session can, e.g., be immediately terminated.

Activity recording system **24** is utilized to store IP addresses and timing information for sessions occurring with the target server **32**. This information is stored in an IP address/userid table **36**, which can then be used by IP address activity analysis system **26**. IP address/userid table **36** may be implemented in any format that can track userids, login time, and IP addresses.

One possible implementation would involve a hash tree that indexes IP addresses such that each address points to a linked list of userids (and associated login times) that have logged onto the particular IP address. FIG. **3** depicts an illustrative embodiment of such an implementation involving three linked lists **60** for IP Addr **1**, IP Addr **2**, and IP Addr **3**. As can be seen for the first IP address **62** (Addr **1**), there have been two logins **64** by userid **9** and userid **2**. For each login, there is an associated login time.

IP address activity analysis system **26** (FIG. **1**) is utilized to examine the IP address/userid table **36** to identify any IP addresses that have an unusually large number of logins during some predefined time period. For example, threshold values may be utilized that would be customizable by the target organization based on their tolerance for risk (much like a biometric system or intrusion detection system must be tuned to minimize false positives while not overlooking real attacks). These observed values and associated thresholds could be expressed as follows:

N=number of userids logging in from the given IP address

Nt=threshold of acceptable number of userids logging in from any given IP address

T=time interval over which logins from a given IP address have been attempted

Tt=time interval threshold triggering suspicion

Then, the following algorithm could be implemented:

If N>Nt and T>Tt then
suspect MITM attack
otherwise
proceed with login and record details.

It is understood that the above is for illustrative purposes only, and more complex algorithms could be utilized, e.g., ones that take into account time of day, past usage history, analysis of the specific userids, etc.

Countermeasure system **28** is utilized to respond to a suspected MITM attack by taking some defensive action. Any type of countermeasure could be implemented. For instance, in a case where a login is being attempted from a suspicious IP address, the login can simply be denied. In other cases, if a first session is currently underway and a large number of additional sessions are started from the same IP address, the first session could be terminated. In these cases, the suspicious IP address could be added to the black list **34**. In still further cases, suspect IP address can be simply outputted to a user for further investigation.

FIG. **4** depicts a flow diagram of a process for implementing MITM defense system **18** (FIG. **1**) for a login procedure. At S**1**, a login request is received and the userid, password and IP address are recorded at S**2**. At S**3**, the login credentials are subjected to verification, and if they fail, an authentication failure message is returned at S**18**, and the session is terminated at S**19**. If the login credentials succeed, then an MITM white list is searched to locate the incoming IP address at S**5**.

If it is found at S6, then defense processing is skipped and the session is allowed to continue at S7. Otherwise, an MITM black list is searched for the incoming IP address at step S8. If the IP address is found in the black list at S9, then an MITM failure message is returned at S15, and the session is terminated at S17.

If the incoming IP address is not found in the black list, then a search is made for previous login attempts from the incoming IP address at S10. At S11, the number of userids originating from the IP address are determined, and the activity level is determined at S12 (e.g., how many during a particular time period). At S13, the number and activity level are compared against threshold values, and if exceeded, the IP address is added to the black list at S16, an MITM failure message is returned at S15, and the session is terminated at S17. If the threshold values are not exceeded, then at S14, the IP address, userid, and time are recorded in the IP address userid table, and the login continues.

Referring again to FIG. 1, it is understood that computer system 10 may be implemented as any type of computing infrastructure. Computer system 10 generally includes a processor 12, input/output (I/O) 14, memory 16, and bus 17. The processor 12 may comprise a single processing unit, or be distributed across one or more processing units in one or more locations, e.g., on a client and server. Memory 16 may comprise any known type of data storage and/or transmission media, including magnetic media, optical media, random access memory (RAM), read-only memory (ROM), a data cache, a data object, etc. Moreover, memory 16 may reside at a single physical location, comprising one or more types of data storage, or be distributed across a plurality of physical systems in various forms.

I/O 14 may comprise any system for exchanging information to/from an external resource. External devices/resources may comprise any known type of external device, including a monitor/display, speakers, storage, another computer system, a hand-held device, keyboard, mouse, voice recognition system, speech output system, printer, facsimile, pager, etc. Bus 17 provides a communication link between each of the components in the computer system 10 and likewise may comprise any known type of transmission link, including electrical, optical, wireless, etc. Although not shown, additional components, such as cache memory, communication systems, system software, etc., may be incorporated into computer system 10.

Access to computer system 10 may be provided over a network such as the Internet, a local area network (LAN), a wide area network (WAN), a virtual private network (VPN), etc. Communication could occur via a direct hardwired connection (e.g., serial port), or via an addressable connection that may utilize any combination of wireline and/or wireless transmission methods. Moreover, conventional network connectivity, such as Token Ring, Ethernet, WiFi or other conventional communications standards could be used. Still yet, connectivity could be provided by conventional TCP/IP sockets-based protocol. In this instance, an Internet service provider could be used to establish interconnectivity. Further, as indicated above, communication could occur in a client-server or server-server environment.

It should be appreciated that the teachings of the present invention could be offered as a business method on a subscription or fee basis. For example, a computer system 10 comprising a MITM defense system 18 could be created, maintained and/or deployed by a service provider that offers the functions described herein for customers. That is, a service provider could offer to deploy or provide the ability to identify and respond to MITM attacks as described above.

It is understood that in addition to being implemented as a system and method, the features may be provided as a program product stored on a computer-readable medium, which when executed, enables computer system 10 to provide an MITM defense system 18. To this extent, the computer-readable medium may include program code, which implements the processes and systems described herein. It is understood that the term "computer-readable medium" comprises one or more of any type of physical embodiment of the program code. In particular, the computer-readable medium can comprise program code embodied on one or more portable storage articles of manufacture (e.g., a compact disc, a magnetic disk, a tape, etc.), on one or more data storage portions of a computing device, such as memory 16 and/or a storage system, and/or as a data signal traveling over a network (e.g., during a wired/wireless electronic distribution of the program product).

As used herein, it is understood that the terms "program code" and "computer program code" are synonymous and mean any expression, in any language, code or notation, of a set of instructions that cause a computing device having an information processing capability to perform a particular function either directly or after any combination of the following: (a) conversion to another language, code or notation; (b) reproduction in a different material form; and/or (c) decompression. To this extent, program code can be embodied as one or more types of program products, such as an application/software program, component software/a library of functions, an operating system, a basic I/O system/driver for a particular computing and/or I/O device, and the like. Further, it is understood that terms such as "component" and "system" are synonymous as used herein and represent any combination of hardware and/or software capable of performing some function(s).

The block diagrams in the figures illustrate the architecture, functionality, and operation of possible implementations of systems, methods and computer program products according to various embodiments of the present invention. In this regard, each block in the block diagrams may represent a module, segment, or portion of code, which comprises one or more executable instructions for implementing the specified logical function(s). It should also be noted that the functions noted in the blocks may occur out of the order noted in the figures. For example, two blocks shown in succession may, in fact, be executed substantially concurrently, or the blocks may sometimes be executed in the reverse order, depending upon the functionality involved. It will also be noted that each block of the block diagrams can be implemented by special purpose hardware-based systems which perform the specified functions or acts, or combinations of special purpose hardware and computer instructions.

Although specific embodiments have been illustrated and described herein, those of ordinary skill in the art appreciate that any arrangement which is calculated to achieve the same purpose may be substituted for the specific embodiments shown and that the invention has other applications in other environments. This application is intended to cover any adaptations or variations of the present invention. The following claims are in no way intended to limit the scope of the invention to the specific embodiments described herein.

What is claimed is:

1. A system for defending against man in the middle (MITM) attacks directed at a target server, comprising:

an activity recording system that records an incoming IP address, user id, and time of each session occurring with the target server;

a list checking system for performing the following:

comparing a single incoming IP address with a white list; and

comparing the single incoming IP address with a black list after the comparing of the single incoming IP address with the white list in the case that the single incoming IP address is not present on the white list;

an activity analysis system that performs the following after the list checking system compares the single incoming IP address with the black list, in the case that the single incoming IP address is not present on the black list:

searches for records of a previous login attempt from the single incoming IP address;

determines a number of user ids occurring from the single incoming IP address during a predefined time period;

compares the number of user ids occurring from the single incoming IP address to a predefined threshold number of user ids specific to the predefined time period; and

identifies the single incoming IP address as a suspect IP address in response to the number of user ids occurring from the single incoming IP address exceeding the threshold within the predefined time period,

wherein the activity analysis system includes a first value N that represents a number of sessions along with a threshold value Nt and a second value T and its associated threshold value Tt that represents a time frame, and wherein if there are more than N sessions with the single incoming IP address during a time period less than T, the single incoming IP address is identified as a suspect IP address; and

a countermeasure system for taking action against the suspect IP address.

2. The system of claim **1**, wherein the countermeasure system causes a login session to fail.

3. The system of claim **1**, wherein the countermeasure system causes a session to terminate in response to the identifying of the single incoming IP address as a suspect address.

4. The system of claim **1**, wherein the countermeasure system causes the suspect IP address to be outputted.

5. A computer program product stored on a non-transitory computer readable medium, which when executed includes program instructions for defending against man in the middle (MITM) attacks directed at a target server, the program product comprising:

program instructions for recording an incoming IP address, user id, and time of each session occurring with the target server;

program instructions for comparing the incoming IP address with a white list;

program instructions for comparing the incoming IP address with a black list after the comparing of the incoming IP address with the white list in the case that the incoming IP address is not present on the white list;

program instructions for searching for records of a previous login attempt from the single incoming IP address;

program instructions for identifying suspect IP addresses by determining a number of user ids occurring from the single incoming IP address during a predefined time period after the comparing of the incoming IP address with the black list, in the case that the single incoming IP address is not present on the black list;

program instructions for comparing the number of user ids occurring from the single incoming IP address to a predefined threshold number of user ids specific to the predefined time period;

program instructions for identifying the single incoming IP address as a suspect IP address in response to the number of user ids occurring from the single incoming IP address exceeding the threshold within the predefined time period,

wherein a first value N represents a number of sessions along with a threshold value Nt and a second value T and its associated threshold value Tt represents a time frame, and wherein if there are more than N sessions with the single incoming IP address during a time period less than T, the single incoming IP address is identified as a suspect IP address; and

program instructions for taking defensive action against the suspect IP address.

6. The program product of claim **5**, wherein the defensive action causes a login session to fail.

7. The program product of claim **5**, wherein the defensive action causes a session to terminate in response to the identifying of the single incoming IP address as a suspect address.

8. The program product of claim **5**, wherein the defensive action causes the suspect IP address to be outputted.

9. A computer-implemented method performed on at least one computing device for defending against man in the middle (MITM) attacks directed at a target server, the method comprising:

recording an incoming IP address, user id, and time of each session occurring with the target server using the at least one computing device;

comparing the incoming IP address with a white list;

comparing the incoming IP address with a black list after the comparing of the incoming IP address with the white list in the case that the incoming IP address is not present on the white list;

searching for records of a previous login attempt from the single incoming IP address;

identifying suspect IP addresses by determining a number of user ids occurring from the single incoming IP address during a predefined time period after the comparing of the incoming IP address with the black list, in the case that the single incoming IP address is not present on the black list;

comparing the number of user ids occurring from the single incoming IP address to a predefined threshold number of user ids specific to the predefined time period;

identifying the single incoming IP address as a suspect IP address in response to the number of user ids occurring from the single incoming IP address exceeding the threshold within the predefined time period,

wherein a first value N represents a number of sessions along with a threshold value Nt and a second value T and its associated threshold value Tt represents a time frame, and wherein if there are more than N sessions with the single incoming IP address during a time period less than T, the single incoming IP address is identified as a suspect IP address; and

taking defensive action against the suspect IP address using the at least one computing device.

10. The method of claim **9**, wherein the defensive action causes a login session to fail.

11. The method of claim **9**, wherein the defensive action causes a session to terminate in response to the identifying of the single incoming IP address as a suspect address.

12. The method of claim 9, wherein the defensive action causes the suspect IP address to be outputted.

13. A method for deploying a system for defending against man in the middle (MITM) attacks directed at a target server, comprising:

providing a computer infrastructure being operable to:

record an incoming IP address, user id, and time of each session occurring with the target server;

compare the incoming IP address with a white list;

compare the incoming IP address with a black list after the comparing of the incoming IP address with the white list in the case that the incoming IP address is not present on the white list;

search for records of a previous login attempt from the single incoming IP address;

identify suspect IP addresses by determining a number of user ids occurring from the single incoming IP address during a predefined time period after the comparing of the incoming IP address with the black list, in the case that the single incoming IP address is not present on the black list;

compare the number of user ids occurring from the single incoming IP address to a predefined threshold number of user ids specific to the predefined time period;

identify the single incoming IP address as a suspect IP address in response to the number of user ids occurring from the single incoming IP address exceeding the threshold within the predefined time period,

wherein a first value N represents a number of sessions along with a threshold value Nt and a second value T and its associated threshold value Tt represents a time frame, and wherein if there are more than N sessions with the single incoming IP address during a time period less than T, the single incoming IP address is identified as a suspect IP address; and

take defensive action against the suspect IP address.

* * * * *

US008522349B2

(12) **United States Patent**
Crume

(10) **Patent No.: US 8,522,349 B2**
(45) **Date of Patent: Aug. 27, 2013**

(54) **DETECTING AND DEFENDING AGAINST MAN-IN-THE-MIDDLE ATTACKS**

(75) Inventor: **Jeffrey L. Crume**, Raleigh, NC (US)

(73) Assignee: **International Business Machines Corporation**, Armonk, NY (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **13/432,956**

(22) Filed: **Mar. 28, 2012**

(65) **Prior Publication Data**

US 2012/0185938 A1 Jul. 19, 2012

Related U.S. Application Data

(63) Continuation of application No. 11/753,673, filed on May 25, 2007.

(51) **Int. Cl.**
G06F 11/00 (2006.01)

(52) **U.S. Cl.**
USPC **726/23**; 726/3; 726/13; 726/26; 726/34; 713/170; 713/176; 713/177; 709/220; 709/230; 705/51

(58) **Field of Classification Search**
USPC 726/22–23, 13, 27; 713/131
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,310,720	A	1/1982	Check, Jr.
5,046,082	A	9/1991	Zicker et al.
5,068,894	A	11/1991	Hoppe
5,323,465	A	6/1994	Avarne
5,457,737	A	10/1995	Wen
5,491,752	A	2/1996	Kaufman et al.
5,497,411	A	3/1996	Pellerin
5,647,388	A	7/1997	Butler, Jr. et al.
5,657,388	A	8/1997	Weiss
5,684,950	A	11/1997	Dare et al.
5,701,339	A	12/1997	Suda
5,749,052	A	5/1998	Hidem et al.
5,841,871	A	11/1998	Pinkas
5,842,124	A	11/1998	Kenagy et al.

(Continued)

FOREIGN PATENT DOCUMENTS

DE	10317176	11/2004
EP	1119147 A1	7/2001

(Continued)

OTHER PUBLICATIONS

Justin Ma, Beyond Blacklists, Jul. 2009, ACM, vol. 9 , pp. 1245-153.*

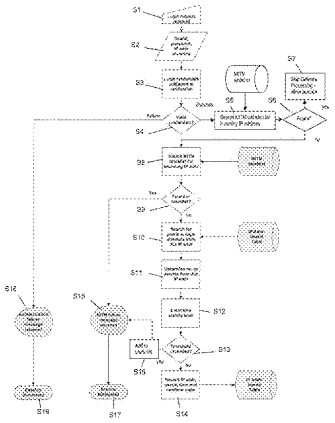
(Continued)

Primary Examiner — Nathan Flynn
Assistant Examiner — Viral Lakhia
(74) *Attorney, Agent, or Firm* — Douglas A. Lashmit; Hoffman Warnick LLC

(57) **ABSTRACT**

A system, method and program product for defending against man in the middle (MITM) attacks directed at a target server. A system is provided that includes an activity recording system that records an incoming IP address, userid, and time of each session occurring with the target server; an activity analysis system that identifies suspect IP addresses by determining if an unacceptable number of sessions are occurring from a single incoming IP address during a predefined time period; and a countermeasure system for taking action against suspect IP addresses.

22 Claims, 4 Drawing Sheets



(56) **References Cited**

U.S. PATENT DOCUMENTS

5,892,902 A 4/1999 Clark
5,953,422 A 9/1999 Angelo et al.
5,971,272 A 10/1999 Hsiao
6,000,031 A 12/1999 Bingaman et al.
6,169,890 B1 1/2001 Vatanen
6,278,863 B1 8/2001 Mabrouki
6,308,268 B1 10/2001 Audebert
6,324,271 B1 11/2001 Sawyer et al.
6,330,608 B1 12/2001 Stiles
6,334,056 B1 12/2001 Holmes et al.
6,338,140 B1 1/2002 Owens et al.
6,349,134 B1 2/2002 Katz
6,385,729 B1 5/2002 DiGiorgio et al.
6,387,729 B2 5/2002 Eng et al.
6,393,468 B1 5/2002 McGee
6,400,726 B1 6/2002 Piret et al.
6,466,780 B1 10/2002 Geiselman et al.
6,535,726 B1 3/2003 Johnson
6,584,309 B1 6/2003 Whigham
6,687,241 B1 2/2004 Goss
6,707,915 B1 3/2004 Jobst et al.
6,731,731 B1 5/2004 Ueshima
6,993,658 B1 1/2006 Engberg et al.
6,993,663 B1 1/2006 Paya et al.
7,007,301 B2 * 2/2006 Crosbie et al. 726/23
7,024,688 B1 4/2006 Faccin et al.
7,028,179 B2 4/2006 Anderson et al.
7,058,796 B2 6/2006 Lynn et al.
7,058,968 B2 6/2006 Rowland et al.
7,100,204 B1 8/2006 Myllymaki et al.
7,133,662 B2 11/2006 Bravo et al.
7,142,840 B1 11/2006 Geddes et al.
7,221,949 B2 5/2007 Clough
7,290,278 B2 10/2007 Cahill et al.
7,317,693 B1 * 1/2008 Roesch et al. 370/252
7,324,976 B2 1/2008 Gupta et al.
7,337,431 B1 2/2008 Barnes et al.
7,357,310 B2 4/2008 Calabrese et al.
7,360,248 B1 4/2008 Kanevsky et al.
7,376,431 B2 5/2008 Niedermeyer
7,379,921 B1 5/2008 Kiliccote
7,380,708 B1 6/2008 Kiliccote
7,447,494 B2 11/2008 Law et al.
7,480,805 B1 1/2009 Gnech et al.
7,491,308 B2 2/2009 Talieh et al.
7,519,989 B2 4/2009 Lin et al.
7,533,414 B1 5/2009 Reed et al.
7,536,634 B2 5/2009 Green et al.
7,540,022 B2 5/2009 Barari et al.
7,594,270 B2 9/2009 Church et al.
7,600,676 B1 10/2009 Rados et al.
7,609,625 B2 10/2009 Wei et al.
7,623,458 B2 11/2009 Ayyagari et al.
7,624,447 B1 11/2009 Horowitz et al.
7,665,128 B2 2/2010 Yang
7,673,334 B2 3/2010 Takemori et al.
7,715,823 B2 5/2010 Bravo et al.
7,716,742 B1 5/2010 Roesch et al.
7,757,285 B2 7/2010 Kubota et al.
7,765,584 B2 7/2010 Roskind
7,779,465 B2 8/2010 Baker et al.
7,823,199 B1 10/2010 Rathi et al.
7,840,993 B2 11/2010 Ganesan et al.
7,845,004 B2 11/2010 Bardsley et al.
7,886,346 B2 2/2011 Sandhu et al.
7,926,108 B2 4/2011 Rand et al.
7,930,540 B2 * 4/2011 Ahuja et al. 713/167
7,954,150 B2 5/2011 Croft et al.
7,975,293 B2 7/2011 Yoshida et al.
8,019,995 B2 9/2011 van Bemmel
8,024,567 B2 9/2011 Han
8,050,658 B2 11/2011 Hong
8,060,915 B2 11/2011 Voice et al.
8,136,150 B2 3/2012 Hayler et al.
8,150,370 B2 4/2012 Dempo et al.
8,151,327 B2 4/2012 Eisen
8,181,248 B2 5/2012 Oh et al.
8,201,217 B1 6/2012 Begen et al.
8,254,542 B2 8/2012 Frederick
8,281,375 B2 10/2012 Von Krogh
8,285,639 B2 10/2012 Eden et al.
8,296,823 B2 10/2012 Schubert
8,301,877 B2 10/2012 Grajek et al.
8,302,180 B1 * 10/2012 Gudov et al. 726/13
8,302,187 B1 10/2012 Gupta et al.
2001/0054155 A1 12/2001 Hagan et al.
2002/0069165 A1 6/2002 O'Neil
2002/0091931 A1 7/2002 Quick et al.
2002/0095588 A1 7/2002 Shigematsu et al.
2002/0178070 A1 11/2002 Leveridge
2002/0178370 A1 11/2002 Gurevich et al.
2003/0014315 A1 1/2003 Jaalinoja et al.
2003/0154382 A1 8/2003 Vicard
2003/0172272 A1 9/2003 Ehlers et al.
2004/0148520 A1 * 7/2004 Talpade et al. 713/201
2004/0152446 A1 8/2004 Saunders et al.
2004/0198329 A1 10/2004 Vasa
2005/0015624 A1 * 1/2005 Ginter et al. 713/201
2005/0018618 A1 1/2005 Mualem et al.
2005/0022020 A1 1/2005 Fremberg
2005/0060535 A1 3/2005 Bartas
2005/0075070 A1 4/2005 Crilly, Jr.
2005/0182958 A1 8/2005 Pham et al.
2005/0187934 A1 8/2005 Motsinger et al.
2005/0188423 A1 8/2005 Motsinger et al.
2005/0210251 A1 9/2005 Nyberg et al.
2006/0021031 A1 * 1/2006 Leahy et al. 726/22
2006/0036690 A1 2/2006 O'Neil
2006/0094403 A1 5/2006 Norefors et al.
2006/0095955 A1 5/2006 Vong et al.
2006/0288411 A1 * 12/2006 Garg et al. 726/22
2007/0015492 A1 1/2007 Bravo et al.
2007/0067828 A1 3/2007 Bychkov
2007/0083606 A1 * 4/2007 Malik et al. 709/207
2007/0084913 A1 4/2007 Weston
2007/0107050 A1 5/2007 Selvarajan
2007/0136573 A1 6/2007 Steinberg
2007/0136808 A1 6/2007 Xiong
2007/0143851 A1 6/2007 Nicodemus et al.
2007/0186099 A1 8/2007 Beck et al.
2007/0234426 A1 * 10/2007 Khanolkar et al. 726/23
2007/0261112 A1 * 11/2007 Todd et al. 726/11
2007/0266257 A1 11/2007 Camaisa et al.
2008/0028447 A1 1/2008 O'Malley et al.
2008/0172730 A1 7/2008 Sandhu et al.
2008/0181380 A1 7/2008 Gustave et al.
2008/0189776 A1 8/2008 Constable
2008/0209275 A1 8/2008 Kwan et al.
2008/0270301 A1 10/2008 Jones et al.
2008/0281737 A1 11/2008 Fajardo
2008/0318548 A1 12/2008 Bravo et al.
2009/0037329 A1 2/2009 Coppinger et al.
2009/0077637 A1 3/2009 Santos et al.
2009/0094682 A1 4/2009 Sage et al.
2009/0095588 A1 4/2009 Thomas
2009/0104889 A1 4/2009 Lotvonen et al.
2009/0106138 A1 4/2009 Smith et al.
2009/0300738 A1 12/2009 Dewe et al.
2010/0024017 A1 1/2010 Ashfield et al.
2010/0051686 A1 3/2010 Obi
2010/0095351 A1 * 4/2010 Liu et al. 726/3
2010/0269162 A1 10/2010 Bravo et al.
2011/0015449 A1 1/2011 Pendleton et al.
2011/0039237 A1 * 2/2011 Skare 434/118
2011/0138483 A1 6/2011 Bravo et al.
2011/0197070 A1 8/2011 Mizrah
2011/0225647 A1 * 9/2011 Dilley et al. 726/14
2011/0277024 A1 11/2011 Begley et al.
2011/0289576 A1 11/2011 Cheng
2012/0011066 A1 1/2012 Telle et al.
2012/0149334 A1 6/2012 Zhang et al.
2012/0204241 A1 8/2012 Varsavsky et al.
2012/0264405 A1 10/2012 Bravo et al.
2012/0272331 A1 * 10/2012 Lemaster et al. 726/27

FOREIGN PATENT DOCUMENTS

GB	2456509	A	7/2009
JP	10334048		12/1998
JP	10341224		12/1998
JP	2001111545		4/2001
WO	0109808	A1	8/2001
WO	2004079499	A2	9/2004
WO	2006103387	A1	10/2006
WO	2008147353	A1	12/2008

OTHER PUBLICATIONS

U.S. Appl. No. 11/753,673, filed Mar. 25, 2007, Office Action dated Dec. 22, 2011.
U.S. Appl. No. 11/753,673, filed Mar. 25, 2007, Office Action dated Oct. 8, 2010.
U.S. Appl. No. 11/753,673, filed Mar. 25, 2007, Office Action dated Apr. 15, 2010.
Lee et al., "A Resilient Packet-Forwarding Scheme against Maliciously Packet-Dropping Nodes in Sensor Networks", ACM 2006.
Kaafar et al., "Real attacks on virtual networks: Vivaldi out of tune", ACM 2006.
Juels, Ari, "Strengthening EPC Tags Against Cloning", ACM 2005.
Deng et al., "Defending Against Redirect Attacks in Mobile IP", ACM 2002.
Lakhia, U.S. Appl. No. 11/753,673, Notice of Allowance, Jun. 18, 2012, 11 pages.
Gee, U.S. Appl. No. 13/084,823, Office Action, IBMC-0395, Mar. 11, 2013, 8 pages.
Leung, "Depress Phishing by CAPTCHA with OTP", Department of Information Engineering The Chinese University of Hong Kong, IEEE 2009, 6 pgs.
Kopsidas et al., "Voice Interactive Personalized Security (VoIPSEC) protocol: Fortify Internet telephony by providing end-to-end security through inbound key exchange and biometric verification", 2006 IEEE, 10 pgs.
Koo et al., "VoIP Interception in P2P SIP Environment", 2010 IEEEE, vol. 1, pp. 331-334.
Megeed, U.S. Appl. No. 12/423,928, Office Action 1, IBMC-0326, 21 pages, Aug. 25, 2011.
Megeed, U.S. Appl. No. 12/423,928, Final Office Action 1, IBMC-0326, 20 pages, Nov. 10, 2011.
Megeed, U.S. Appl. No. 12/423,928, Office Action 2, IBMC-0326, 20 pages, Jun. 8, 2012.
Megeed, U.S. Appl. No. 12/423,928, Notice of Allowance 1, IBMC-0326, 10 pages, Sep. 25, 2012.
Megeed, U.S. Appl. No. 12/423,928, Notice of Allowance 2, IBMC-0326, 19 pages, Dec. 4, 2012.
Bibbee, U.S. Appl. No. 11/765,193, Office Action 1, 15 pages, Feb. 18, 2010.
Bibbee, U.S. Appl. No. 11/765,193, Office Action 2, 14 pages, Nov. 29, 2010.
Bibbee, U.S. Appl. No. 11/765,193, Office Action 3, 18 pages, Sep. 19, 2011.
Bibbee, U.S. Appl. No. 11/765,193, Final Office Action 1, 15 pages, Jul. 30, 2010.
Bibbee, U.S. Appl. No. 11/765,193, Final Office Action 2, 17 pages, May 12, 2011.
Bibbee, U.S. Appl. No. 11/765,193, Final Office Action 3, 18 pages, Apr. 16, 2012.
Tran, U.S. Appl. No. 11/524,340, Office Action, 9 pages, Jul. 29, 2009.
Tran, U.S. Appl. No. 11/524,340, Office Action, 19 pages, Oct. 31, 2008.
Tran, U.S. Appl. No. 11/524,340, Notice of Allowance, 11 pages, Dec. 29, 2009.
Tran, U.S. Appl. No. 11/524,340, Office Action, 7 pages, Apr. 29, 2009.
Tran, U.S. Appl. No. 11/524,340, Office Action, 22 pages, May 27, 2008.
Alicherry et al., "DoubleCheck: Multi-ath Verification Against Man-in-the-Middle Attack", IEEE 2009, pp. 557-563.
Kumaraguru et al., "Getting Users to Pay Attention to Anti-Phishing Education: Evaluation of Retention and Transfer", APWG eCrime Researchers Summit, Oct. 4-5, 2007, Pittsburgh, PA pp. 70-81.
Adida, "BeamAuth: Two-Factor Web Authentication with a Bookmark", CCS '07, Oct. 29-Nov. 2, 2007, Alexandria, VA, ACM 978-1-59593-703-2/07/0010, pp. 48-57.
Nassar et al., "Holistic VoIP Intrusion Detection and Prevention System", IPTCOMM '07, ACM 2007, pp. 1-9.
Stoll et al., "Sesame: Informing User Security Decisions with System Visualization", CHI 2008 Proceedings, Am I Safe, Apr. 5-10, 2008, Florence, Italy, pp. 1045-1054.
Bonzo, U.S. Appl. No. 11/776,619, Notice of Allowance, Apr. 29, 2010, 10 pages.
Bonzo, U.S. Appl. No. 11/776,619, Office Action, Sep. 30, 2009, 12 pages.
"Prevent Online Banking Fraud", Dec. 7, 2010, http://www.phonefactor.com/products/transaction-verification, 1 pages.
Geneiatakis et al., "Survey of Security Vulnerabilities in Session Initiation Protocol", 3rd Quarter 2006, vol. 8, No. 3, IEEE Communications Surveys & Tutorials, pp. 68-81.
Almeida, U.S. Appl. No. 12/630,875, Office Action, IBMC-0353, Mar. 1, 2012, 17 pages.
Almeida, U.S. Appl. No. 12/630,875, Office Action, IBMC-0353, Aug. 30, 2012, 14 pages.
Almeida, U.S. Appl. No. 12/630,875, Notice of Allowance, IBMC-0353, Dec. 20, 2012, 7 pages.
Lakhia, U.S. Appl. No. 11/753,673, Office Action, Jan. 8, 2013, 14 pages.
Bibbee, U.S. Appl. No. 11/765,193, Examiner's Answer, RSW920070138US1, Apr. 16, 2013, 20 pages.
Almeida, U.S. Appl. No. 12/630,875, Office Action, Apr. 17, 2013, 40 pages.
Lakhia, U.S. Appl. No. 11/753,673, Notice of Allowance & Fees Due, dated May 10, 2013, 28 pages.

* cited by examiner

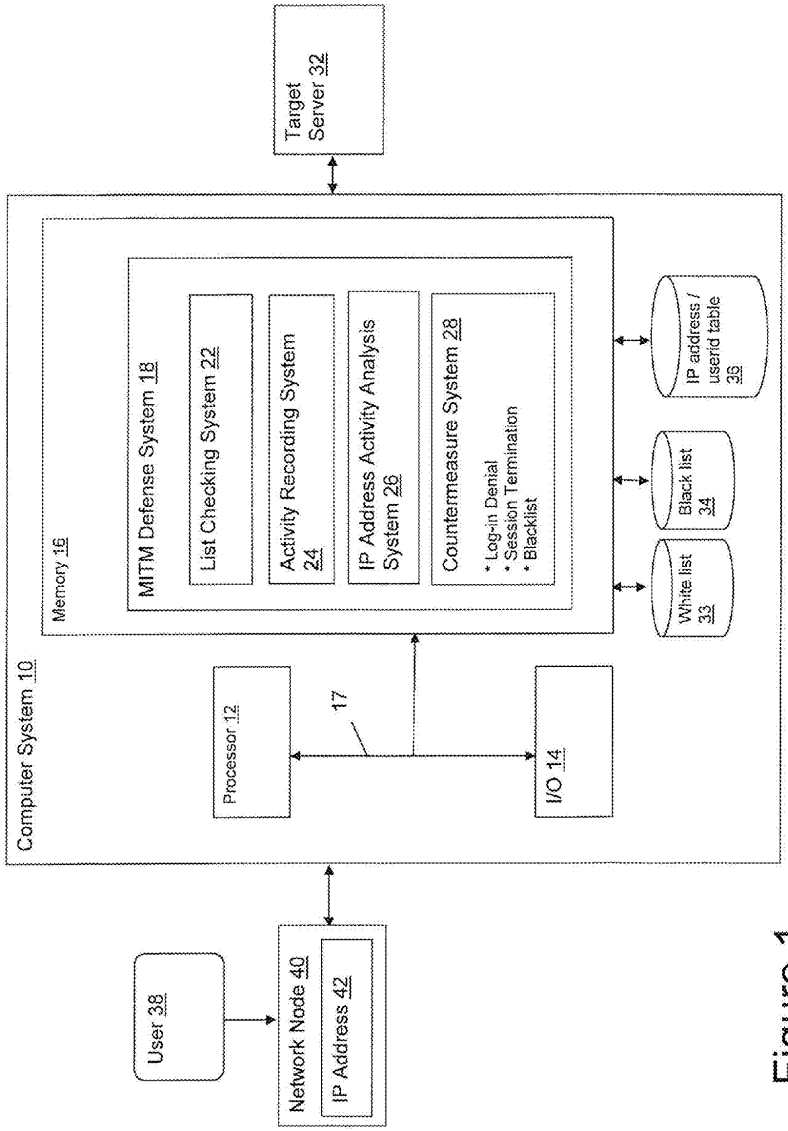

Target Server 32
Computer System 10
Memory 16
MITM Defense System 18
List Checking System 22
Activity Recording System 24
IP Address Activity Analysis System 26
Countermeasure System 28
• Log-in Denial
• Session Termination
• Blacklist
IP address / userid table 36
Black list 34
White list 33
Processor 12
17
I/O 14
User 38
Network Node 40
IP Address 42

Figure 1

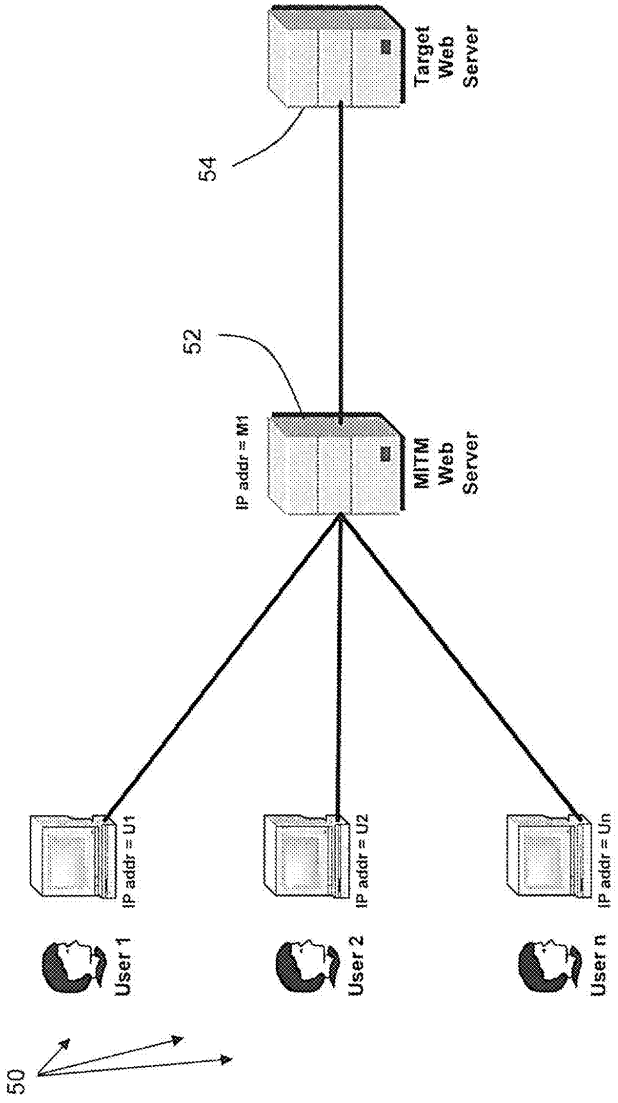

Target Web Server
54
52
IP addr = M1
MITM Web Server
IP addr = U1
IP addr = U2
IP addr = Un
User 1
User 2
User n
50

Figure 2

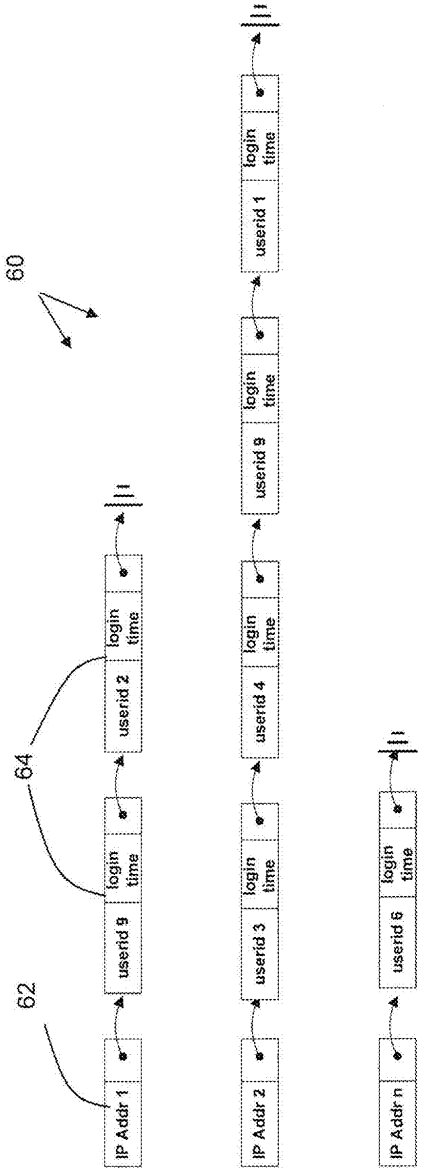

60
62
64
IP Addr 1
userid 9
login time
userid 2
login time
IP Addr 2
userid 3
login time
userid 4
login time
userid 9
login time
userid 1
login time
IP Addr n
userid 6
login time

Figure 3

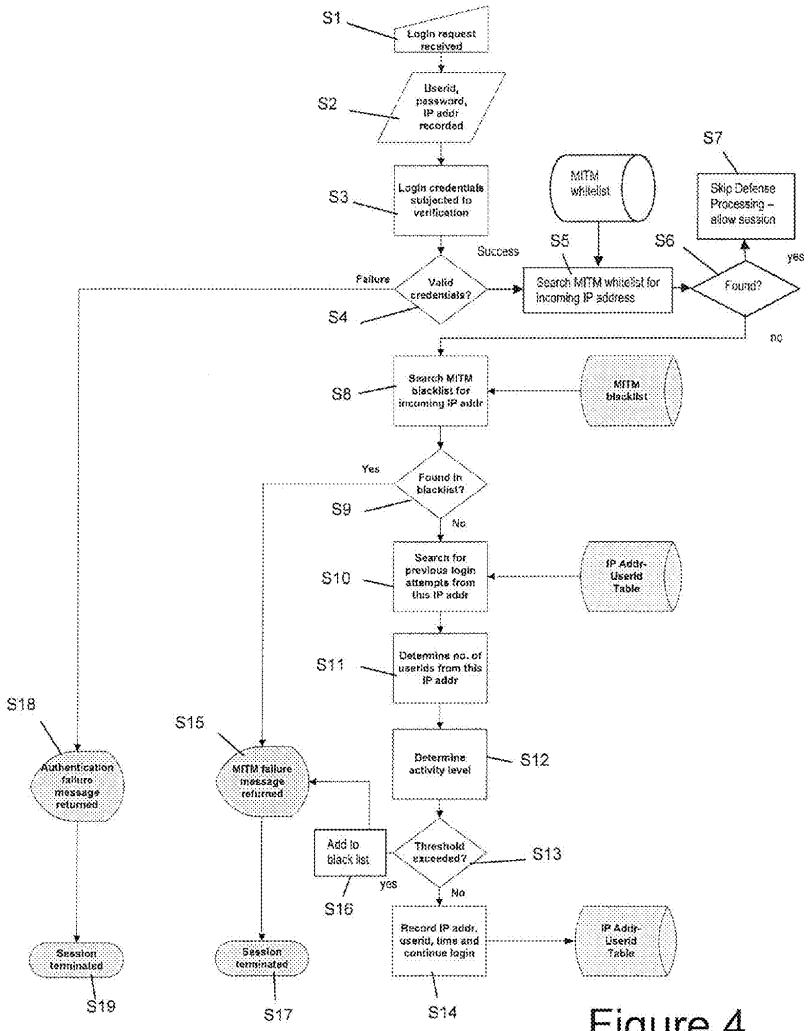

S1
Login request received
S2
Userid, password, IP addr recorded
S3
Login credentials subjected to verification
S4
Valid credentials?
Failure
Success
S5
Search MITM whitelist for incoming IP address
MITM whitelist
S6
Found?
yes
no
S7
Skip Defense Processing – allow session
S8
Search MITM blacklist for incoming IP addr
MITM blacklist
S9
Found in blacklist?
Yes
No
S10
Search for previous login attempts from this IP addr
IP Addr-Userid Table
S11
Determine no. of userids from this IP addr
S12
Determine activity level
S13
Threshold exceeded?
yes
No
S14
Record IP addr, userid, time and continue login
IP Addr-Userid Table
S15
MITM failure message returned
Add to black list
S16
S17
Session terminated
S18
Authentication failure message returned
S19
Session terminated

Figure 4

DETECTING AND DEFENDING AGAINST MAN-IN-THE-MIDDLE ATTACKS

CROSS-REFERENCE TO RELATED APPLICATION

This Application is a continuation of currently pending U.S. patent application Ser. No. 11/753,673, which was filed on May 25, 2007 and is hereby incorporated by reference.

FIELD OF THE INVENTION

This disclosure relates generally to protecting the integrity of network communications, and more particularly to a system and method of detecting and defending against man-in-the-middle (MITM) attacks.

BACKGROUND

One of the most difficult network-based attacks to defend against is that of a class known as "man-in-the-middle" (MITM) attacks. These scenarios involve the insertion by an attacker of an untrusted node into a session path. This MITM attack node then impersonates the identity of one session partner to the other while having access to and control over all transmissions between the partners resulting in the potential for eavesdropping and unauthorized modification of session traffic. These attacks are particularly effective when combined with "phishing" techniques which trick an end user into giving up personal information that later results in identity theft or fraud.

FIG. **2** depicts an example of an MITM attack, in which a plurality of users **50** are unsuspectingly engaged in sessions with an MITM Web server **52**, which sits between users **50** and the legitimate target Web server **54**. In this case, MITM Web server **52** has lured users **50** into believing that they are engaging in a session with the target Web server **54**.

Banks and other financial institutions have been particularly hard hit by these attacks as customers are lured into logging onto a malicious MITM node thinking they are connecting to their bank, while the MITM node interacts with the legitimate web site and relays information to the user making the ruse even more believable. It is this last aspect that is particularly distressing to banks as they do not have a good way to detect that they are dealing with an MITM node rather than directly with their customer. Because the attacker's MITM machine looks and acts just like a real end user, the MITM machine acts as a conduit for sensitive information such as userids and passwords and, potentially, for conducting transactions.

While digital certificates could provide a reasonable measure of protection in such an instance, they have thus far proven to be difficult and expensive to deploy and manage across a large end user base especially when those users may have limited technical skills and may also be highly mobile, using many different nodes to conduct transactions.

Another increasingly popular defense is to use "strong" authentication mechanisms such as security tokens, smart cards or biometrics to ensure that the end user is who they claim to be. The problem with these defenses is that in the MITM case, the digitized authentication data is simply passed directly through the intermediate node making it unnecessary for the attacker to actually possess the token, smart card or physical characteristic being measured.

Finally, another technique for alerting end users that they are being lured into logging into a bogus Web site involves the presentation of a graphical image pre-selected by the user.

During login, if the user does not see the image they selected during registration (something which only they and the legitimate Web site should know), then they know to abort the authentication process. However, in an MITM case, the target Web site presents the image to the MITM node thinking it is the end user and the MITM node relays this image to the real end user leading them to believe that the attack node is legitimate.

BRIEF SUMMARY OF THE INVENTION

The present invention relates to a system, method and program product for detecting man in the middle attacks. In one embodiment, there is a system for defending against man in the middle (MITM) attacks directed at a target server, comprising: an activity recording system that records an incoming IP address, userid, and time of each session occurring with the target server; an activity analysis system that identifies suspect IP addresses by determining if an unacceptable number of sessions are occurring from a single incoming IP address during a predefined time period; and a countermeasure system for taking action against suspect IP addresses.

In a second embodiment, there is a computer program product stored on a computer readable medium, which when executed includes program instructions for defending against man in the middle (MITM) attacks directed at a target server, the program product comprising: program instructions for recording an incoming IP address, userid, and time of each session occurring with the target server; program instructions for identifying suspect IP addresses by determining if an unacceptable number of sessions are occurring from a single incoming IP address during a predefined time period; and program instructions for taking defensive action against suspect IP addresses.

In a third embodiment, there is method for defending against man in the middle (MITM) attacks directed at a target server, comprising: recording an incoming IP address, userid, and time of each session occurring with the target server; identifying suspect IP addresses by determining if an unacceptable number of sessions are occurring from a single incoming IP address during a predefined time period; and taking defensive action against suspect IP addresses.

In a fourth embodiment, there is a method for deploying a system for defending against man in the middle (MITM) attacks directed at a target server, comprising: providing a computer infrastructure being operable to: record an incoming IP address, userid, and time of each session occurring with the target server; identify suspect IP addresses by determining if an unacceptable number of sessions are occurring from a single incoming IP address during a predefined time period; and take defensive action against suspect IP addresses.

MITM attacks of the sort described herein share a detectable characteristic that can be used to predict to some reasonable certainty that an attack is taking place. Once detected, defensive action can be taken, such as sending a message that will be relayed by the MITM node to the user informing the user of the potential vulnerability and ending the session.

The observable characteristic shared by successful MITM attacks is that to the target server it will appear that a large number of different end users have for no apparent reason begun logging on from the same IP address, i.e., the address of the MITM proxy. If, for instance, certain definable thresholds were exceeded such as N number of userids from a single, previously unknown address within a specific interval of time, then further investigation or even automated defenses would be warranted.

Some advantages to this technique include: the thresholds can be tuned to suit the risk tolerance of the target organization; detection can be automated; countermeasures can be automated to limit further damage; automated detection and response allows for constant vigilance by providing a continuous, 24×7 defense; the basic technique can be extended beyond web spoofing/phishing attacks to other types of MITM scenarios; the more "successful" the attacker is at luring victims, the more likely the attack will be detected and repelled

The illustrative aspects of the present invention are designed to solve the problems herein described and other problems not discussed.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other features of this invention will be more readily understood from the following detailed description of the various aspects of the invention taken in conjunction with the accompanying drawings.

FIG. **1** depicts a computer system having an MITM defense system in accordance with an embodiment of the present invention.

FIG. **2** depicts an example of an MITM attack.

FIG. **3** depicts an example of an IP address/userid table in accordance with an embodiment of the present invention.

FIG. **4** depicts a flow diagram showing an illustrative implementation of an embodiment of the present invention.

The drawings are merely schematic representations, not intended to portray specific parameters of the invention. The drawings are intended to depict only typical embodiments of the invention, and therefore should not be considered as limiting the scope of the invention. In the drawings, like numbering represents like elements.

DETAILED DESCRIPTION

FIG. **1** depicts a computer system **10** that provides an MITM defense system **18** for a target server **32** communicating with a user **38** via network node **40**. In particular, MITM defense system **18** analyzes the IP address **42** of network node **40** to determine whether network node **40** is a legitimate node associated with user **38** or an MITM server that has interposed itself between the user **38** and target server **32**. Note that in this illustrative embodiment, computer system **10** containing MITM defense system **18** is shown separated from target server **32**. However, it is understood that MITM defense system **18** may be integrated with target server **32** in a single system.

As noted above, an observable characteristic shared by successful MITM attacks is that it will appear to the target server **32** that a large number of different end users have for no apparent reason begun logging on from the same IP address **42**, i.e., the address of the MITM server. While this behavior alone will not conclusively indicate malicious activity, identifying and analyzing such behavior can allow for further investigation or countermeasures to be taken. For instance, definable thresholds involving the allowed number of user IDs from a single, previously unknown address within a specific interval of time can be put in place to identify suspicious activity. When a threshold is exceeded, then further investigation or even automated defenses can be implemented.

As shown in this illustrative embodiment, MITM defense system **18** includes a list checking system **22**, an activity recording system **24**, an IP address activity analysis system **26**, and a countermeasure system **28**. List checking system **22** is utilized to compare an incoming IP address **42** with either or both a white list **33** and a black list **34**. The white list **33** may include a list of known IP addresses that are valid, and need not be analyzed (e.g., the IP address associated with a known legitimate proxy, etc.). The black list **34** may include a list of known IP addresses that are invalid (e.g., sites that are known to have caused attacks in the past). When an IP address **42** is found on the black list **34**, the session can, e.g., be immediately terminated.

Activity recording system **24** is utilized to store IP addresses and timing information for sessions occurring with the target server **32**. This information is stored in an IP address/userid table **36**, which can then be used by IP address activity analysis system **26**. IP address/userid table **36** may be implemented in any format that can track userids, login time, and IP addresses.

One possible implementation would involve a hash tree that indexes IP addresses such that each address points to a linked list of userids (and associated login times) that have logged onto the particular IP address. FIG. **3** depicts an illustrative embodiment of such an implementation involving three linked lists **60** for IP Addr **1**, IP Addr **2**, and IP Addr **3**. As can be seen for the first IP address **62** (Addr **1**), there have been two logins **64** by userid **9** and userid **2**. For each login, there is an associated login time.

IP address activity analysis system **26** (FIG. **1**) is utilized to examine the IP address/userid table **36** to identify any IP addresses that have an unusually large number of logins during some predefined time period. For example, threshold values may be utilized that would be customizable by the target organization based on their tolerance for risk (much like a biometric system or intrusion detection system must be tuned to minimize false positives while not overlooking real attacks). These observed values and associated thresholds could be expressed as follows:

N=number of userids logging in from the given IP address

Nt=threshold of acceptable number of userids logging in from any given IP address

T=time interval over which logins from a given IP address have been attempted

Tt=time interval threshold triggering suspicion

Then, the following algorithm could be implemented:

If N>Nt and T>Tt then
suspect MITM attack
otherwise
proceed with login and record details.

It is understood that the above is for illustrative purposes only, and more complex algorithms could be utilized, e.g., ones that take into account time of day, past usage history, analysis of the specific userids, etc.

Countermeasure system **28** is utilized to respond to a suspected MITM attack by taking some defensive action. Any type of countermeasure could be implemented. For instance, in a case where a login is being attempted from a suspicious IP address, the login can simply be denied. In other cases, if a first session is currently underway and a large number of additional sessions are started from the same IP address, the first session could be terminated. In these cases, the suspicious IP address could be added to the black list **34**. In still further cases, suspect IP address can be simply outputted to a user for further investigation.

FIG. **4** depicts a flow diagram of a process for implementing MITM defense system **18** (FIG. **1**) for a login procedure. At S**1**, a login request is received and the userid, password and IP address are recorded at S**2**. At S**3**, the login credentials are subjected to verification, and if they fail, an authentication failure message is returned at S**18**, and the session is terminated at S**19**. If the login credentials succeed, then an MITM

white list is searched to locate the incoming IP address at S5. If it is found at S6, then defense processing is skipped and the session is allowed to continue at S7. Otherwise, an MITM black list is searched for the incoming IP address at step S8. If the IP address is found in the black list at S9, then an MITM failure message is returned at S15, and the session is terminated at S17.

If the incoming IP address is not found in the black list, then a search is made for previous login attempts from the incoming IP address at S10. At S11, the number of userids originating from the IP address are determined, and the activity level is determined at S12 (e.g., how many during a particular time period). At S13, the number and activity level are compared against threshold values, and if exceeded, the IP address is added to the black list at S16, an MITM failure message is returned at S15, and the session is terminated at S17. If the threshold values are not exceeded, then at S14, the IP address, userid, and time are recorded in the IP address userid table, and the login continues.

Referring again to FIG. 1, it is understood that computer system 10 may be implemented as any type of computing infrastructure. Computer system 10 generally includes a processor 12, input/output (I/O) 14, memory 16, and bus 17. The processor 12 may comprise a single processing unit, or be distributed across one or more processing units in one or more locations, e.g., on a client and server. Memory 16 may comprise any known type of data storage and/or transmission media, including magnetic media, optical media, random access memory (RAM), read-only memory (ROM), a data cache, a data object, etc. Moreover, memory 16 may reside at a single physical location, comprising one or more types of data storage, or be distributed across a plurality of physical systems in various forms.

I/O 14 may comprise any system for exchanging information to/from an external resource. External devices/resources may comprise any known type of external device, including a monitor/display, speakers, storage, another computer system, a hand-held device, keyboard, mouse, voice recognition system, speech output system, printer, facsimile, pager, etc. Bus 17 provides a communication link between each of the components in the computer system 10 and likewise may comprise any known type of transmission link, including electrical, optical, wireless, etc. Although not shown, additional components, such as cache memory, communication systems, system software, etc., may be incorporated into computer system 10.

Access to computer system 10 may be provided over a network such as the Internet, a local area network (LAN), a wide area network (WAN), a virtual private network (VPN), etc. Communication could occur via a direct hardwired connection (e.g., serial port), or via an addressable connection that may utilize any combination of wireline and/or wireless transmission methods. Moreover, conventional network connectivity, such as Token Ring, Ethernet, WiFi or other conventional communications standards could be used. Still yet, connectivity could be provided by conventional TCP/IP sockets-based protocol. In this instance, an Internet service provider could be used to establish interconnectivity. Further, as indicated above, communication could occur in a client-server or server-server environment.

It should be appreciated that the teachings of the present invention could be offered as a business method on a subscription or fee basis. For example, a computer system 10 comprising a MITM defense system 18 could be created, maintained and/or deployed by a service provider that offers the functions described herein for customers. That is, a service provider could offer to deploy or provide the ability to identify and respond to MITM attacks as described above.

It is understood that in addition to being implemented as a system and method, the features may be provided as a program product stored on a computer-readable medium, which when executed, enables computer system 10 to provide an MITM defense system 18. To this extent, the computer-readable medium may include program code, which implements the processes and systems described herein. It is understood that the term "computer-readable medium" comprises one or more of any type of physical embodiment of the program code. In particular, the computer-readable medium can comprise program code embodied on one or more portable storage articles of manufacture (e.g., a compact disc, a magnetic disk, a tape, etc.), on one or more data storage portions of a computing device, such as memory 16 and/or a storage system, and/or as a data signal traveling over a network (e.g., during a wired/wireless electronic distribution of the program product).

As used herein, it is understood that the terms "program code" and "computer program code" are synonymous and mean any expression, in any language, code or notation, of a set of instructions that cause a computing device having an information processing capability to perform a particular function either directly or after any combination of the following: (a) conversion to another language, code or notation; (b) reproduction in a different material form; and/or (c) decompression. To this extent, program code can be embodied as one or more types of program products, such as an application/software program, component software/a library of functions, an operating system, a basic I/O system/driver for a particular computing and/or I/O device, and the like. Further, it is understood that terms such as "component" and "system" are synonymous as used herein and represent any combination of hardware and/or software capable of performing some function(s).

The block diagrams in the figures illustrate the architecture, functionality, and operation of possible implementations of systems, methods and computer program products according to various embodiments of the present invention. In this regard, each block in the block diagrams may represent a module, segment, or portion of code, which comprises one or more executable instructions for implementing the specified logical function(s). It should also be noted that the functions noted in the blocks may occur out of the order noted in the figures. For example, two blocks shown in succession may, in fact, be executed substantially concurrently, or the blocks may sometimes be executed in the reverse order, depending upon the functionality involved. It will also be noted that each block of the block diagrams can be implemented by special purpose hardware-based systems which perform the specified functions or acts, or combinations of special purpose hardware and computer instructions.

Although specific embodiments have been illustrated and described herein, those of ordinary skill in the art appreciate that any arrangement which is calculated to achieve the same purpose may be substituted for the specific embodiments shown and that the invention has other applications in other environments. This application is intended to cover any adaptations or variations of the present invention. The following claims are in no way intended to limit the scope of the invention to the specific embodiments described herein.

What is claimed is:

1. A system comprising:

at least one computing device configured to defend against man in the middle (MITM) attacks directed at a target server, the at least computing device comprising:

an activity recording system that records an incoming IP address, user id, and time of each session occurring with the target server;

a list checking system for performing the following:

comparing a single incoming IP address with a white list; and

comparing the single incoming IP address with a black list after the comparing of the single incoming IP address with the white list and after determining that the single incoming IP address is not present on the white list;

an activity analysis system that performs the following after the list checking system compares the single incoming IP address with the black list, and after determining that the single incoming IP address is not present on the black list:

searches for records of a previous login attempt from the single incoming IP address;

determines a number of user ids occurring from the single incoming IP address during a predefined time period;

compares the number of user ids occurring from the single incoming IP address to a predefined threshold number of user ids specific to the predefined time period; and

identifies the single incoming IP address as a suspect IP address in response to the number of user ids occurring from the single incoming IP address exceeding the threshold within the predefined time period; and

a countermeasure system for taking action against the suspect IP address.

2. The system of claim **1**, wherein the activity analysis system includes a first value N that represents a number of sessions along with a threshold value Nt and a second value T and its associated threshold value Tt that represents a time frame, and wherein if there are more than N sessions with the single incoming IP address during a time period less than T, the single incoming IP address is identified as a suspect IP address.

3. The system of claim **1**, wherein the countermeasure system causes a login session to fail.

4. The system of claim **1**, wherein the countermeasure system causes a session to terminate in response to the identifying of the single incoming IP address as a suspect address.

5. The system of claim **1**, wherein the countermeasure system causes the suspect IP address to be outputted.

6. A computer program product stored on a non-transitory computer readable medium, which when executed includes program instructions for defending against man in the middle (MITM) attacks directed at a target server, the program product comprising:

program instructions for recording an incoming IP address, user id, and time of each session occurring with the target server;

program instructions for comparing the incoming IP address with a white list;

program instructions for comparing the incoming IP address with a black list after the comparing of the incoming IP address with the white list and after determining that the incoming IP address is not present on the white list;

program instructions for searching for records of a previous login attempt from the incoming IP address;

program instructions for identifying suspect IP addresses by determining a number of user ids occurring from the single incoming IP address during a predefined time period after the comparing of the incoming IP address with the black list, and after determining that the single incoming IP address is not present on the black list;

program instructions for comparing the number of user ids occurring from the single incoming IP address to a predefined threshold number of user ids specific to the predefined time period;

program instructions for identifying the single incoming IP address as a suspect IP address in response to the number of user ids occurring from the single incoming IP address exceeding the threshold within the predefined time period; and

program instructions for taking defensive action against the suspect IP address.

7. The program product of claim **6**, wherein a first value N represents a number of sessions along with a threshold value Nt and a second value T and its associated threshold value Tt represents a time frame, and wherein if there are more than N sessions with the single incoming IP address during a time period less than T, the single incoming IP address is identified as a suspect IP address.

8. The program product of claim **6**, wherein the defensive action causes a login session to fail.

9. The program product of claim **6**, wherein the defensive action causes a session to terminate in response to the identifying of the single incoming IP address as a suspect address.

10. The program product of claim **6**, wherein the defensive action causes the suspect IP address to be outputted.

11. A computer-implemented method performed on at least one computing device for defending against man in the middle (MITM) attacks directed at a target server, the method comprising:

recording an incoming IP address, user id, and time of each session occurring with the target server using the at least one computing device;

comparing the incoming IP address with a white list;

comparing the incoming IP address with a black list after the comparing of the incoming IP address with the white list and after determining that the incoming IP address is not present on the white list;

searching for records of a previous login attempt from the incoming IP address;

identifying suspect IP addresses by determining a number of user ids occurring from the single incoming IP address during a predefined time period after the comparing of the incoming IP address with the black list, and after determining that the single incoming IP address is not present on the black list;

comparing the number of user ids occurring from the single incoming IP address to a predefined threshold number of user ids specific to the predefined time period;

identifying the single incoming IP address as a suspect IP address in response to the number of user ids occurring from the single incoming IP address exceeding the threshold within the predefined time period; and

taking defensive action against the suspect IP address using the at least one computing device.

12. The method of claim **11**, wherein a first value N represents a number of sessions along with a threshold value Nt and a second value T and its associated threshold value Tt represents a time frame, and wherein if there are more than N sessions with the single incoming IP address during a time period less than T, the single incoming IP address is identified as a suspect IP address.

13. The method of claim 11, wherein the defensive action causes a login session to fail.

14. The method of claim 11, wherein the defensive action causes a session to terminate in response to the identifying of the single incoming IP address as a suspect address.

15. The method of claim 11, wherein the defensive action causes the suspect IP address to be outputted.

16. A computer-implemented method for deploying a system for defending against man in the middle (MITM) attacks directed at a target server, comprising:

providing at least one computing device being operable to:

record an incoming IP address, user id, and time of each session occurring with the target server;

compare the incoming IP address with a white list;

compare the incoming IP address with a black list after the comparing of the incoming IP address with the white list and after determining that the incoming IP address is not present on the white list;

search for records of a previous login attempt from the incoming IP address;

identify suspect IP addresses by determining a number of user ids occurring from the incoming IP address during a predefined time period after the comparing of the incoming IP address with the black list, and after determining that the single incoming IP address is not present on the black list;

compare the number of user ids occurring from the single incoming IP address to a predefined threshold number of user ids specific to the predefined time period;

identify the single incoming IP address as a suspect IP address in response to the number of user ids occurring from the single incoming IP address exceeding the threshold within the predefined time period; and

take defensive action against the suspect IP address.

17. The method of claim 1, wherein the activity recording system records the incoming IP address, the user id, and the time of each session occurring with the target server in a hash tree that indexes the incoming IP address with the user id and the time of each session.

18. The method of claim 17, wherein the activity analysis system searches for the records of the previous login attempt from the single incoming IP address and determines the number of user ids occurring from the single incoming IP address using the hash tree.

19. The computer program product of claim 6, wherein the incoming IP address, the user id, and the time of each session occurring with the target server are recorded in a hash tree that indexes the incoming IP address with the user id and the time of each session.

20. The computer program product of claim 19, wherein the program instructions for identifying suspect IP addresses determines the number of user ids occurring from the single incoming IP address during the predefined time period using the hash tree.

21. The computer implemented method of claim 11, wherein the incoming IP address, the user id, and the time of each session occurring with the target server are recorded in a hash tree that indexes the incoming IP address with the user id and the time of each session.

22. The computer implemented method of claim 21, wherein the identifying of suspect IP addresses determines the number of user ids occurring from the single incoming IP address during the predefined time period using the hash tree.

* * * * *

9.8 System for Detecting the Presence of Rogue Domain Name Service Providers through Passive Monitoring

(12) **United States Patent**
Crume

(10) **Patent No.: US 9,225,731 B2**
(45) **Date of Patent: Dec. 29, 2015**

(54) **SYSTEM FOR DETECTING THE PRESENCE OF ROGUE DOMAIN NAME SERVICE PROVIDERS THROUGH PASSIVE MONITORING**

(75) Inventor: **Jeffery L. Crume**, Raleigh, NC (US)

(73) Assignee: **International Business Machines Corporation**, Armonk, NY (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 473 days.

(21) Appl. No.: **13/479,412**

(22) Filed: **May 24, 2012**

(65) **Prior Publication Data**

US 2013/0318170 A1 Nov. 28, 2013

(51) **Int. Cl.**
H04L 29/12 (2006.01)
H04L 29/06 (2006.01)
H04L 12/26 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 63/1408*** (2013.01); ***H04L 61/1511*** (2013.01); ***H04L 63/1483*** (2013.01); *H04L 43/00* (2013.01)

(58) **Field of Classification Search**
CPC H04L 61/1511; H04L 61/15; H04L 63/04; H04L 43/00; H04L 63/1483
USPC 709/245
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

7,706,267 B2 * 4/2010 Ford et al. 370/230
7,756,933 B2 7/2010 Reshef et al.
7,823,202 B1 10/2010 Nucci et al.
7,873,993 B2 1/2011 King
8,055,768 B2 11/2011 Saunderson et al.
8,069,483 B1 11/2011 Matlock
8,312,541 B2 11/2012 Levy-Abegnoli et al.
8,370,933 B1 * 2/2013 Buckler 726/22
2004/0030796 A1 2/2004 Cooper et al.
2004/0111640 A1 6/2004 Baum
2006/0176822 A1 * 8/2006 Doyle et al. 370/241
2006/0253612 A1 11/2006 Cheshire
2007/0186276 A1 8/2007 McRae et al.
2007/0271220 A1 * 11/2007 Carter 707/2
2008/0060054 A1 3/2008 Srivastava
2008/0147837 A1 * 6/2008 Klein et al. 709/223
2008/0307516 A1 12/2008 Levy-Abegnoli et al.
2009/0327487 A1 12/2009 Olson et al.
(Continued)

OTHER PUBLICATIONS

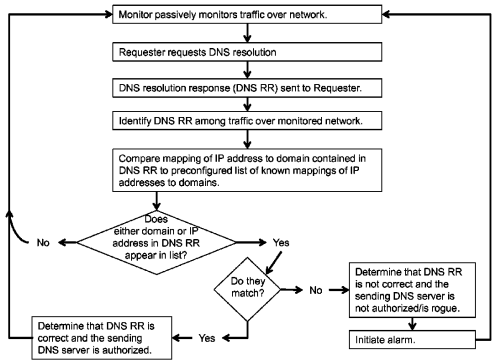
Torres-Diaz, Office Action Communication for U.S. Appl. No. 13/479,418 dated Nov. 26, 2013, 11 pages.
(Continued)

Primary Examiner — Uzma Alam
(74) *Attorney, Agent, or Firm* — Douglas A. Lashmit; Hoffman Warnick LLC

(57) **ABSTRACT**

A method, system, and computer program product embodied in a computer readable storage medium are disclosed for identifying a rogue domain name service (DNS) server. Embodiments include passively monitoring traffic on a target network; and identifying a DNS resolution response in the traffic on the network. The DNS resolution response includes a mapping of a domain to an internet protocol (IP) address. The DNS resolution response is compared with a preconfigured list of known mappings of domains to IP addresses. Based on the results of the comparison, it can be determined whether the DNS resolution response is correct. In cases where the DNS resolution response is incorrect, the provider of the DNS resolution response is a rogue DNS server.

15 Claims, 5 Drawing Sheets



(56) **References Cited**

U.S. PATENT DOCUMENTS

2010/0031362	A1	2/2010	Himberger et al.	
2010/0142709	A1	6/2010	Robert et al.	
2010/0262688	A1	10/2010	Hussain et al.	
2010/0291943	A1	11/2010	Mihaly et al.	
2011/0106919	A1	5/2011	Mazur et al.	
2011/0191455	A1*	8/2011	Gardner	709/223
2011/0208838	A1*	8/2011	Thomas et al.	709/219
2011/0214180	A1	9/2011	Gunawardena	
2011/0231931	A1	9/2011	Ma	
2011/0271345	A1	11/2011	Wolman et al.	
2012/0124087	A1*	5/2012	Malan et al.	707/770
2013/0332986	A1*	12/2013	Sima et al.	726/1
2013/0333038	A1*	12/2013	Chien	726/23

OTHER PUBLICATIONS

Application No. DE 10 2013 208 923.6, Office Action dated Jan. 27, 2014, 12 pags.

Torres-Diaz, Office Action Communication for U.S. Appl. No. 13/479,418 dated May 9, 2013, 17 pages.

Torres-Diaz, Lizbeth, U.S. Appl. No. 13/479,418, Office Action dated Jul. 2, 2014, 13 pages.

Torres-Diaz, Office Action Communication for U.S. Appl. No. 13/479,418 dated Nov. 5, 2014, 14 pages.

* cited by examiner

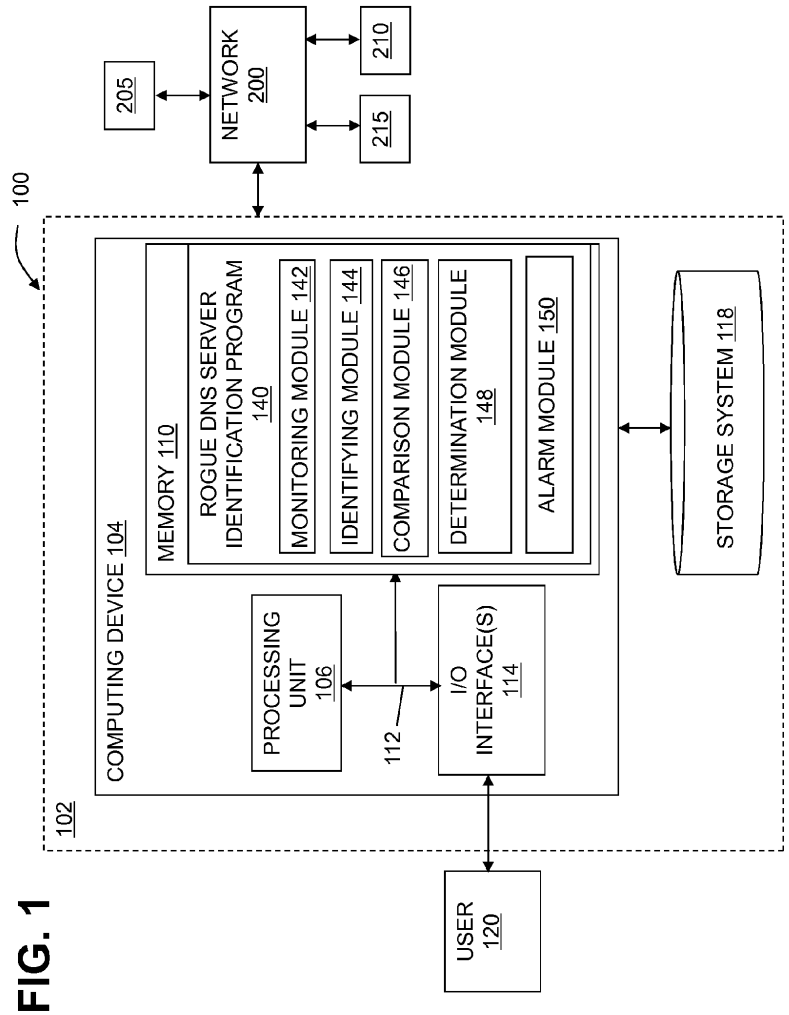

100
205
NETWORK 200
210
215
102
COMPUTING DEVICE 104
MEMORY 110
ROGUE DNS SERVER IDENTIFICATION PROGRAM 140
MONITORING MODULE 142
IDENTIFYING MODULE 144
COMPARISON MODULE 146
DETERMINATION MODULE 148
ALARM MODULE 150
PROCESSING UNIT 106
112
I/O INTERFACE(S) 114
STORAGE SYSTEM 118
USER 120

FIG. 1

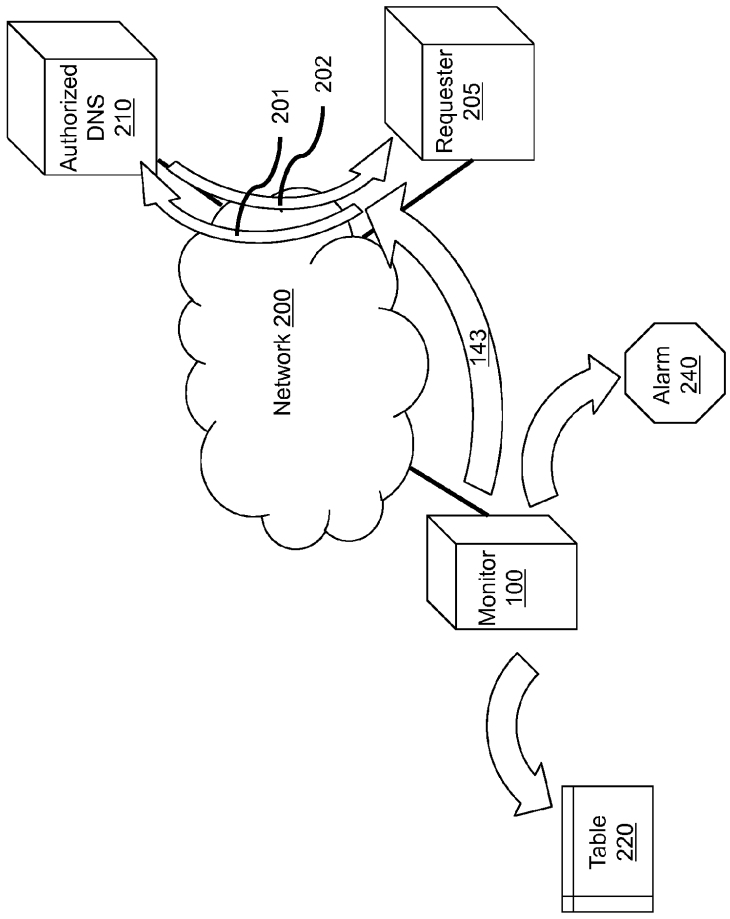

Authorized DNS 210
201
202
Requester 205
Network 200
143
Alarm 240
Monitor 100
Table 220

FIG. 2

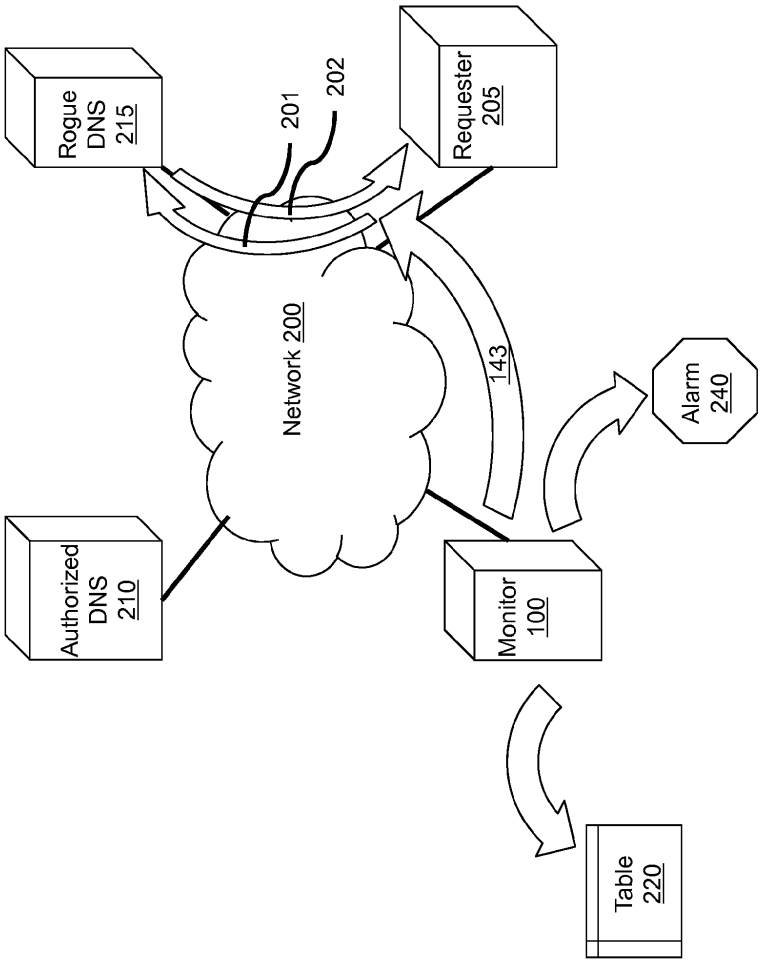

Rogue DNS 215
201
202
Requester 205
Network 200
143
Alarm 240
Authorized DNS 210
Monitor 100
Table 220

FIG. 3

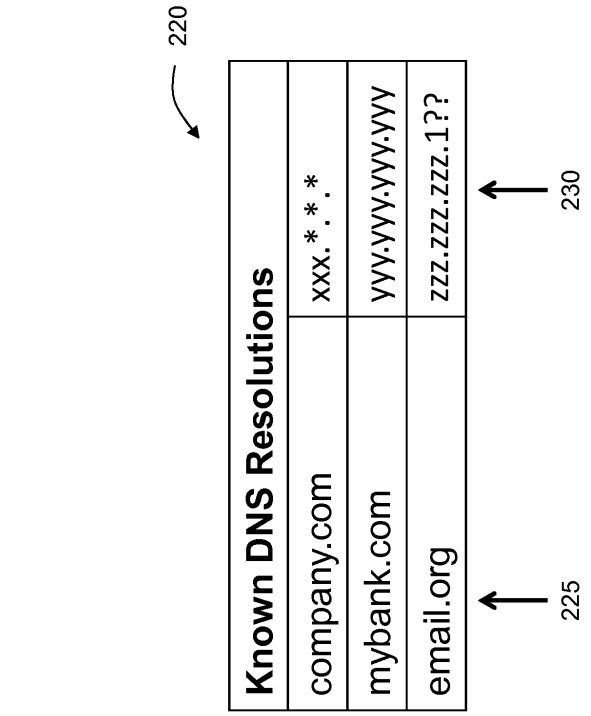

220
Known DNS Resolutions
company.com
xxx.*.*.*
mybank.com
yyy.yyy.yyy.yyy
email.org
zzz.zzz.zzz.1??
225
230

FIG. 4

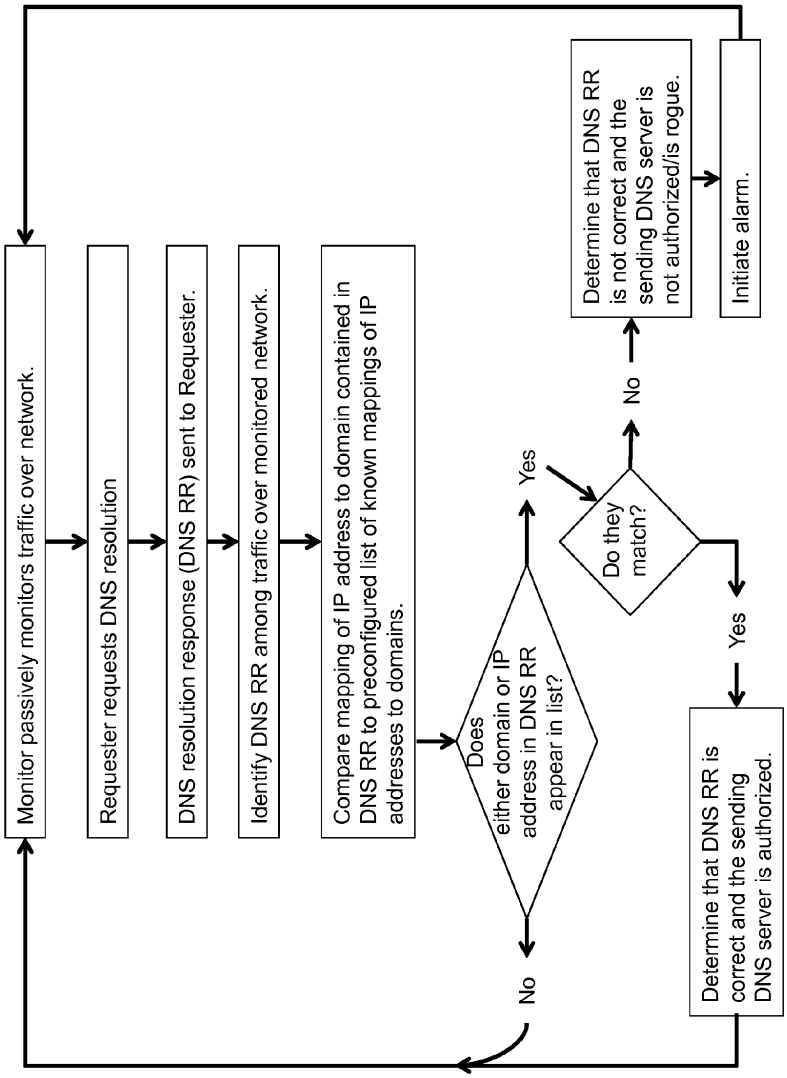

Monitor passively monitors traffic over network.
Requester requests DNS resolution
DNS resolution response (DNS RR) sent to Requester.
Identify DNS RR among traffic over monitored network.
Compare mapping of IP address to domain contained in DNS RR to preconfigured list of known mappings of IP addresses to domains.
Does either domain or IP address in DNS RR appear in list?
Yes
No
Do they match?
Yes
No
Determine that DNS RR is correct and the sending DNS server is authorized.
Determine that DNS RR is not correct and the sending DNS server is not authorized/is rogue.
Initiate alarm.

FIG. 5

SYSTEM FOR DETECTING THE PRESENCE OF ROGUE DOMAIN NAME SERVICE PROVIDERS THROUGH PASSIVE MONITORING

CROSS REFERENCE TO RELATED APPLICATION

This patent application is related to commonly-assigned U.S. patent application Ser. No. 13/479,418, filed concurrently with this application.

TECHNICAL FIELD

The invention relates generally to identifying untrusted or compromised sources for network information. More particularly, the invention relates to identifying rogue DNS servers via passive monitoring.

BACKGROUND

The Domain Name Service (DNS) resolves alphanumeric domain names into numeric IP addresses. This service is provided by a loose collection of servers scattered around the Internet as well as within local Intranets. If, however, the information supplied through this service comes not from an authorized source, but rather, an attacker's system supplying incorrect information or from an authorized source that has been compromised, network traffic could be impeded in a denial of service (DOS) attack or misrouted in a spoofing or man-in-the-middle attack. This could result in sensitive traffic being delivered to untrusted systems or not being delivered at all.

One way that these services could be subverted would be if an attacker set up an "evil twin" WiFi hotspot which impersonates a trusted wireless access point and establishes itself as a man-in-the-middle (MITM), which reroutes network traffic. The MITM can examine and modify all traffic coming into and going out of the rogue network. Another way would be for the attacker to set up a rogue server which hijacks network services by broadcasting to all nodes in the network that it is online and available to process DNS requests. Yet another way would be for an attacker to compromise a trusted DNS server and cause it to produce erroneous results. In many cases, the last server to broadcast will be considered authoritative by other nodes in the network.

One solution for detecting such untrusted or compromised sources of network information is the use of a DNS watcher which performs a "health check" by polling a preconfigured list of trusted DNS servers to verify that they are operational and are returning proper results. There are several drawbacks to this method, however. Polling operations generate additional, superfluous network traffic, and may be discovered by an attacker's reconnaissance of the target network. A polling approach also only verifies whether known DNS servers are performing properly. By virtue of the active nature of polling specific known DNS servers, it is unable to verify the correctness of DNS resolutions returned by hosts other than the known hosts being polled. Since rogue DNS providers would not be known in advance, they would go unchecked by a polling solution.

BRIEF DESCRIPTION

In general, aspects of the present invention provide a passive monitoring solution for identifying a rogue DNS server in a network which does not generate additional network traffic, and is able to monitor DNS resolutions provided by both known and unknown DNS servers.

A first aspect of the disclosure provides a method for identifying a rogue domain name service (DNS) server. The method comprises: passively monitoring traffic on a network; identifying a DNS resolution response in the traffic on the network, wherein the DNS resolution response includes a mapping of a domain to an internet protocol (IP) address; comparing the DNS resolution response with a preconfigured list of known mappings of domains to IP addresses; and determining whether the DNS resolution response is correct based on the comparing.

A second aspect of the disclosure provides a system for identifying a rogue domain name service (DNS) server. The system comprises: a monitoring component for passively monitoring traffic on a network; an identification component for identifying a DNS resolution response in the traffic on the network, wherein the DNS resolution response includes a mapping of a domain to an internet protocol (IP) address; a comparison component for comparing the DNS resolution response with a preconfigured list of known mappings of domains to IP addresses; and a determination component for determining whether the DNS resolution response is correct based on the comparing.

A third aspect of the disclosure provides a computer program product embodied in a computer readable storage medium which, when executed by a computing device, causes the computer system to implement a method for identifying a rogue domain name service (DNS) server. The method comprises: passively monitoring traffic on a network; identifying a DNS resolution response in the traffic on the network, wherein the DNS resolution response includes a mapping of a domain to an internet protocol (IP) address; comparing the DNS resolution response with a preconfigured list of known mappings of domains to IP addresses; and determining whether the DNS resolution response is correct based on the comparing.

These and other aspects, advantages and salient features of the invention will become apparent from the following detailed description, which, when taken in conjunction with the annexed drawings, where like parts are designated by like reference characters throughout the drawings, disclose embodiments of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** shows a data processing system suitable for implementing an embodiment of the invention.

FIG. **2** shows a schematic data flow diagram illustrating monitoring of a network according to an embodiment of the invention.

FIG. **3** shows a schematic data flow diagram illustrating identification of a rogue DNS server according to an embodiment of the invention.

FIG. **4** shows a preconfigured DNS resolution table in accordance with an embodiment of the invention.

FIG. **5** shows a flow chart for a method of identifying a rogue DNS server in accordance with an embodiment of the invention.

The drawings are not necessarily to scale. The drawings are merely schematic representations, not intended to portray specific parameters of the invention. The drawings are intended to depict only typical embodiments of the invention, and therefore should not be considered as limiting the scope of the invention. In the drawings, like numbering represents like elements.

DETAILED DESCRIPTION OF THE INVENTION

As indicated above, aspects of the present invention provide a solution for detecting the presence of rogue DNS servers through the use of a monitor which passively observes the flow of traffic across a network between nodes, and looks for spoofed DNS traffic in that network. In some embodiments, the network may be a local Intranet, and in others, the network may be the Internet.

Turning to the drawings, FIG. **1** shows an illustrative monitor **100** for detecting the presence of rogue DNS servers **215** that may be present in network **200**. To this extent, monitor **100** includes a computer system **102** that can perform a process described herein in order to identify an invalid DNS resolution response from a rogue DNS server **215**. In particular, computer system **102** is shown including a computing device **104** that includes a rogue DNS server identification program **140**, which makes computing device **104** operable to identify a rogue DNS server **215** by performing a process described herein.

Computing device **104** is shown including a processing unit **106** (e.g., one or more processors), a memory **110**, a storage system **118** (e.g., a storage hierarchy), an input/output (I/O) interface component **114** (e.g., one or more I/O interfaces and/or devices), and a communications pathway **112**. In general, processing unit **106** executes program code, such as rogue DNS server identification program **140**, which is at least partially fixed in memory **110**. To this extent, processing unit **106** may comprise a single processing unit, or be distributed across one or more processing units in one or more locations.

Memory **110** can also include local memory, employed during actual execution of the program code, bulk storage (storage **118**), and/or cache memories (not shown) which provide temporary storage of at least some program code in order to reduce the number of times code must be retrieved from bulk storage **118** during execution. As such, memory **110** may comprise any known type of data storage and/or transmission media, including magnetic media, optical media, random access memory (RAM), read-only memory (ROM), a data cache, a data object, etc. Moreover, similar to processing unit **116**, memory **110** may reside at a single physical location, comprising one or more types of data storage, or be distributed across a plurality of physical systems in various forms.

While executing program code, processing component **106** can process data, which can result in reading and/or writing transformed data from/to memory **110** and/or I/O component **114** for further processing. Pathway **112** provides a direct or indirect communications link between each of the components in computer system **102**. I/O interface component **114** can comprise one or more human I/O devices, which enable a human user **120** to interact with computer system **102** and/or one or more communications devices to enable a system user **120** to communicate with computer system **102** using any type of communications link.

To this extent, rogue DNS server identification program **140** can manage a set of interfaces (e.g., graphical user interface(s), application program interface, and/or the like) that enable human and/or system users **120** to interact with rogue DNS server identification program **140**. Further, rogue DNS server identification program **140** can manage (e.g., store, retrieve, create, manipulate, organize, present, etc.) the data, such as data stored in table **220** (FIGS. **2-4**), using any solution.

In any event, computer system **102** can comprise one or more general purpose computing articles of manufacture **104** (e.g., computing devices) capable of executing program code, such as rogue DNS server identification program **140**, installed thereon. As used herein, it is understood that "program code" means any collection of instructions, in any language, code or notation, that cause a computing device having an information processing capability to perform a particular action either directly or after any combination of the following: (a) conversion to another language, code or notation; (b) reproduction in a different material form; and/or (c) decompression. To this extent, rogue DNS server identification program **140** can be embodied as any combination of system software and/or application software. In any event, the technical effect of computer system **102** is to provide processing instructions to computing device **104** in order to identify a rogue DNS server.

Further, rogue DNS server identification program **140** can be implemented using a set of modules **142-150**. In this case, a module **142-150** can enable computer system **102** to perform a set of tasks used by rogue DNS server identification program **140**, and can be separately developed and/or implemented apart from other portions of rogue DNS server identification program **140**. As used herein, the term "component" means any configuration of hardware, with or without software, which implements the functionality described in conjunction therewith using any solution, while the term "module" means program code that enables a computer system **102** to implement the actions described in conjunction therewith using any solution. When fixed in a memory **110** of a computer system **102** that includes a processing component **106**, a module is a substantial portion of a component that implements the actions. Regardless, it is understood that two or more components, modules, and/or systems may share some/all of their respective hardware and/or software. Further, it is understood that some of the functionality discussed herein may not be implemented or additional functionality may be included as part of computer system **102**.

When computer system **102** comprises multiple computing devices **104**, each computing device **104** can have only a portion of rogue DNS server identification program **140** fixed thereon (e.g., one or more modules **142-150**). However, it is understood that computer system **102** and rogue DNS server identification program **140** are only representative of various possible equivalent computer systems that may perform a process described herein. To this extent, in other embodiments, the functionality provided by computer system **102** and rogue DNS server identification program **140** can be at least partially implemented by one or more computing devices that include any combination of general and/or specific purpose hardware with or without program code. In each embodiment, the hardware and program code, if included, can be created using standard engineering and programming techniques, respectively.

When computer system **102** includes multiple computing devices **104**, the computing devices can communicate over any type of communications link. Further, while performing a process described herein, computer system **102** can communicate with one or more other computer systems using any type of communications link. In either case, the communications link can comprise any combination of various types of wired and/or wireless links; comprise any combination of one or more types of networks; and/or utilize any combination of various types of transmission techniques and protocols.

As discussed herein, rogue DNS server identification program **140** enables computer system **102** to implement identification of a rogue DNS server. To this extent, rogue DNS server identification program **140** is shown including a moni-

toring module **142**, an identifying module **144**, a comparison module **146**, a determination module **148**, and an alarm module **150**.

Referring now to FIGS. **2-3**, the network environment **200** in which monitor **100** may be used is depicted. As illustrated, network **200** may include a requester **205**, which may be a client workstation operated by a user or a server. Additional requesters **205** may be included in network **200**, but are omitted from the depiction of network **200** in FIGS. **2-3** for simplicity. Requester **205** may send a DNS resolution request **201** for resolution of a particular host's alphanumeric domain name into a numeric IP address.

As shown in FIG. **2**, under normal operating conditions, in which an attacker is not present in network **200**, DNS resolution request **201** is received and processed by authorized DNS server **210**, which sends DNS resolution response **202**. In that case, DNS resolution response **202** may contain a valid and accurate mapping of domain name to IP address.

In other cases, as shown in FIG. **3**, an attacker's rogue DNS sever **215** may be present in network **200** with the purpose of impersonating another computing system. In this case, DNS resolution request **201** is received and processed by rogue DNS server **215**, and DNS resolution response **202** is provided by rogue DNS server **215**. Such a DNS resolution response **202** may contain an incorrect domain name to IP address mapping, resulting in either misrouting of network traffic in a spoofing attack in which sensitive traffic is delivered to an untrusted system, or impeding of network traffic in a denial of service (DOS) attack.

In either case, monitor **100** is positioned at a strategic point in network **200** such that monitor **100** can observe the flow of network traffic between nodes on network **200**. As discussed above with reference to FIG. **1**, monitor **100** includes modules **142-150**, which when executed by computer system **102**, perform passive monitoring of traffic on network **200**, including, among other network traffic, DNS resolution requests **201** and DNS resolution responses **202**.

Referring concurrently to FIGS. **1-3**, monitoring module **142**, part of monitor **100**, performs monitoring **143** of traffic across network **200**, including DNS resolution requests **201** and DNS resolution responses **202**. Identification component **144** can identify, in the traffic monitored on the network **200**, a DNS resolution response **202**. As mentioned previously, a DNS resolution response **202** includes a mapping of a domain name **225** to an IP address **230** in response to a DNS resolution request **201** sent by requester **205**.

Once a DNS resolution response **202** is identified, comparison module **146** can perform a comparison of the DNS resolution response **202** with the known mappings stored in a preconfigured list of known mappings of domain names and IP addresses contained in a known DNS resolution table **220**. The mappings of domain names to IP addresses contained in table **220** are known to be valid. As shown in FIG. **4**, the IP address **230** stored in table **220** may be expressed as a specific IP address, such as yyy.yyy.yyy.yyy, the IP address of the domain mybank.com. In other embodiments, IP addresses **230** stored in table **200** may be expressed as a range of IP addresses using at least one wild card. A range of IP addresses may be broad, including several wild cards such as, for example, xxx.*.*.*, the IP address range for the domain company.com. In other embodiments the range of IP addresses may be narrower, for example having only one wild card, such as zzz.zzz.zzz.1??, the IP address range for the domain email.org.

According to embodiments of the invention, the list of mapped domain names **225** and IP addresses **230** stored in table **220** need not be an exhaustive list of domains that a user of network **200** may access, or for which requester **205** may request DNS resolutions. Rather, a selected number of hosts may be included in table **220** as a representative sample. In some embodiments, table **220** may include a preconfigured list of domains and their respective IP addresses whose selection for inclusion in table **220** is based on the domain hosting particularly sensitive information accessed by network users. In other embodiments, table **220** may include a preconfigured list of domains and their respective IP addresses whose selection for inclusion in table **220** is based on a high frequency of visits by users of network **200**, and therefore a high likelihood of a large sample pool of DNS resolution requests and responses to monitor.

Referring back to FIGS. **1-3**, determination module **148** performs a determination of whether the DNS resolution response **202** contains a correct and valid mapping of IP address to domain name. This determination is based on the comparison performed by comparison module **146**. Where the mapping in DNS resolution response **202** matches the mapping for the respective domain name stored in table **220**, DNS resolution response **202** is determined to be correct. This would indicate that DNS resolution response **202** may have been sent by authorized DNS server **210** (FIG. **2**). Where the mapping in DNS resolution response **202** does not match the mapping for the respective domain name in table **220**, DNS resolution response **202** is determined to be invalid. This would indicate that DNS resolution response **202** may have been sent by rogue DNS server **215** (FIG. **3**), and may indicate the occurrence of either a spoof or DOS attack. In this case, alarm module **150** sends an alarm **240** to advise requester **205** of the spoofed DNS traffic. In various embodiments, alarm **240** may take the form of a message (email, SMS, etc.), a log entry, or other form of security event notification which documents and draws attention to the suspicious behavior.

The foregoing method is depicted in a flow chart in FIG. **5**. As previously described, a monitor passively monitors traffic over a network. Over this network, a requesting workstation requests a DNS resolution of a particular domain. A DNS resolution response is returned to the Requester over the network by a DNS server. The DNS resolution response is identified by the monitor among the monitored network traffic. Once identified, the mapping of an IP address to a domain contained in the DNS resolution response is compared to a preconfigured list of known mappings of IP addresses to domains. If neither the domain nor the IP address in the DNS resolution response appears in the preconfigured list of known mappings of IP addresses to domains, the monitor simply returns to monitoring the network.

If either the domain or the IP address in the DNS resolution response appears in the preconfigured list of known mappings of IP addresses to domains, the mapping contained in the DNS resolution request is compared to the corresponding mapping in the preconfigured list of known mappings of IP addresses to domains. If the mapping matches, i.e. both the IP address and the respective domain are the same in the DNS resolution response and the preconfigured list of known mappings of IP addresses to domains, then it can be determined that the DNS resolution response is correct and the DNS server that sent it is authorized. If, however, the mapping does not match, i.e., the domain corresponds to different IP addresses in the DNS resolution response and the preconfigured list of known mappings of IP addresses to domains (or the IP address corresponds to different domains in the DNS resolution response and the preconfigured list of known mappings of IP addresses to domains), then it can be determined that the DNS resolution response is invalid. In such a case, it can be concluded that the DNS server that sent it is not

authorized, and may be a rogue DNS server. In this instance, an alarm is initiated, alerting the requester to the security risk.

While shown and described herein as a method and system for identifying a rogue DNS server, it is understood that aspects of the invention further provide various alternative embodiments. For example, in one embodiment, the invention provides a computer program fixed in at least one computer-readable medium, which when executed, enables a computer system to implement identification of a rogue DNS server. To this extent, the computer-readable medium includes program code, such as rogue DNS server identification program **140** (FIG. **1**), which implements some or all of a process described herein. It is understood that the term "computer-readable medium" comprises one or more of any type of tangible medium of expression, now known or later developed, from which a copy of the program code can be perceived, reproduced, or otherwise communicated by a computing device. For example, the computer-readable medium can comprise: one or more portable storage articles of manufacture; one or more memory/storage components of a computing device; paper; and/or the like.

In another embodiment, the invention provides a method of providing a copy of program code, such as rogue DNS server identification program **140** (FIG. **1**), which implements some or all of a process described herein. In this case, a computer system can process a copy of program code that implements some or all of a process described herein to generate and transmit, for reception at a second, distinct location, a set of data signals that has one or more of its characteristics set and/or changed in such a manner as to encode a copy of the program code in the set of data signals. Similarly, an embodiment of the invention provides a method of acquiring a copy of program code that implements some or all of a process described herein, which includes a computer system receiving the set of data signals described herein, and translating the set of data signals into a copy of the computer program fixed in at least one computer-readable medium. In either case, the set of data signals can be transmitted/received using any type of communications link.

In still another embodiment, the invention provides a method of generating a system for identifying a rogue DNS server. In this case, a computer system, such as computer system **102** (FIG. **1**), can be obtained (e.g., created, maintained, made available, etc.) and one or more components for performing a process described herein can be obtained (e.g., created, purchased, used, modified, etc.) and deployed to the computer system. To this extent, the deployment can comprise one or more of: (1) installing program code on a computing device; (2) adding one or more computing and/or I/O devices to the computer system; (3) incorporating and/or modifying the computer system to enable it to perform a process described herein; and/or the like.

As used herein, the terms "first," "second," and the like, do not denote any order, quantity, or importance, but rather are used to distinguish one element from another, and the terms "a" and "an" herein do not denote a limitation of quantity, but rather denote the presence of at least one of the referenced item. The modifier "about" used in connection with a quantity is inclusive of the stated value and has the meaning dictated by the context (e.g., includes the degree of error associated with measurement of the particular quantity). The suffix "(s)" as used herein is intended to include both the singular and the plural of the term that it modifies, thereby including one or more of that term (e.g., the server(s) includes one or more server). Ranges disclosed herein are inclusive and independently combinable (e.g., ranges of "up to about 3 wild cards, or, more specifically, about 1 wild cards to about 3 wild cards," is inclusive of the endpoints and all intermediate values of the ranges of "about 1 wild card to about 2 wild cards," etc.).

The descriptions of the various embodiments of the present invention have been presented for purposes of illustration, but are not intended to be exhaustive or limited to the embodiments disclosed. Many modifications and variations will be apparent to those of ordinary skill in the art without departing from the scope and spirit of the described embodiments. The terminology used herein was chosen to best explain the principles of the embodiments, the practical application or technical improvement over technologies found in the marketplace, or to enable others of ordinary skill in the art to understand the embodiments disclosed herein.

What is claimed is:

1. A method for identifying a rogue domain name service (DNS) server, the method comprising:

passively monitoring traffic on a network;

identifying a DNS resolution response in the traffic on the network, wherein the DNS resolution response includes a mapping of a domain to an internet protocol (IP) address;

comparing the DNS resolution response with a preconfigured list of known mappings of domains to IP addresses, wherein each IP address in the preconfigured list of known mappings of domains to IP addresses is a range of IP addresses expressed using at least one wild card; and

determining whether the DNS resolution response is correct based on the comparing.

2. The method of claim **1**, further comprising sending an alarm in a case in which the DNS resolution response is determined to be incorrect.

3. The method of claim **2**, wherein the alarm comprises at least one of an email message, an SMS message, a log entry, or a security event notification.

4. The method of claim **1**, wherein the preconfigured list of known mappings of domains and IP addresses further includes a preconfigured list of domains most frequently visited by users of a network.

5. The method of claim **1**, wherein the preconfigured list of known mappings of domains and IP addresses further includes a preconfigured list of domains hosting sensitive information accessed by network users.

6. The method of claim **1**, wherein the network includes an intranet.

7. A system for identifying a rogue domain name service (DNS) server comprising:

a monitoring component for passively monitoring traffic on a network;

an identification component for identifying a DNS resolution response in the traffic on the network, wherein the DNS resolution response includes a mapping of a domain to an internet protocol (IP) address;

a comparison component for comparing the DNS resolution response with a preconfigured list of known mappings of domains to IP addresses,

wherein each IP address in the preconfigured list of known mappings of domains to IP addresses is a range of IP addresses expressed using at least one wild card; and

a determination component for determining whether the DNS resolution response is correct based on the comparing.

8. The system of claim **7**, further comprising an alarm component for sending an alarm in a case in which the DNS resolution response is determined to be incorrect.

9. The system of claim 8, wherein the alarm comprises at least one of an email message, an SMS message, a log entry, or a security event notification.

10. The system of claim 7, wherein the preconfigured list of known mappings of domains and IP addresses further includes a preconfigured list of domains most frequently visited by users of a network.

11. The system of claim 7, wherein the preconfigured list of known mappings of domains and IP addresses further includes a preconfigured list of domains hosting sensitive information accessed by network users.

12. The system of claim 7, wherein the network includes an intranet.

13. A computer program product embodied in a computer readable storage device which, when executed by a computing device, causes the computing device to implement a method for identifying a rogue domain name service (DNS) server, the method comprising:

passively monitoring traffic on a network;

identifying a DNS resolution response in the traffic on the network, wherein the DNS resolution response includes a mapping of a domain to an internet protocol (IP) address;

comparing the DNS resolution response with a preconfigured list of known mappings of domains to IP addresses, wherein each IP address in the preconfigured list of known mappings of domains to IP addresses is a range of IP addresses expressed using at least one wild card; and

determining whether the DNS resolution response is correct based on the comparing.

14. The computer program product of claim 13, wherein the method further comprises sending an alarm in a case in which the DNS resolution response is determined to be incorrect.

15. The computer program product of claim 13, wherein the network includes an intranet.

* * * * *

(19) Deutsches Patent- und Markenamt

(10) **DE 10 2013 208 923 B4** 2014.10.16

(12) # Patentschrift

(21) Aktenzeichen: **10 2013 208 923.6**
(22) Anmeldetag: **14.05.2013**
(43) Offenlegungstag: **28.11.2013**
(45) Veröffentlichungstag der Patenterteilung: **16.10.2014**

(51) Int Cl.: ***H04L 12/26*** (2006.01)

(30) Unionspriorität:
13/479,412 24.05.2012 US

(73) Patentinhaber:
International Business Machines Corporation, Armonk, N.Y., US

(74) Vertreter:
Spies Danner & Partner Patentanwälte Partnerschaftsgesellschaft mbB, 80687 München, DE

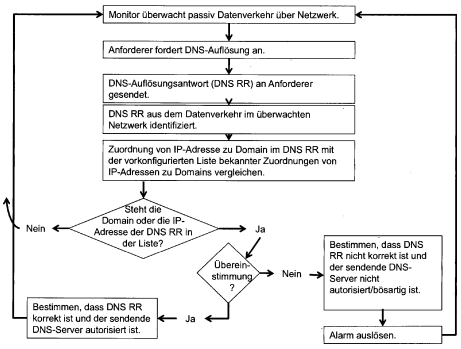
(72) Erfinder:
Crume, Jeffery L., Research Triangle Park, N.C., US

(56) Ermittelter Stand der Technik:

US 2008 / 0 147 837 A1
US 2011 / 0 191 455 A1
US 2012 / 0 124 087 A1

(54) Bezeichnung: **System zum Erfassen des Vorhandenseins eines bösartigen Domain-Name-Service-Providers durch passive Überwachung**

(57) Hauptanspruch: Ein Verfahren zum Identifizieren eines bösartigen Domain Name Service(DNS)-Servers, wobei das Verfahren aufweist:
passives Überwachen von Datenverkehr in einem Netzwerk;
Identifizieren einer DNS-Auflösungsantwort im Datenverkehr im Netzwerk, wobei die DNS-Auflösungsantwort eine Zuordnung einer Domain zu einer Internetprotokoll(IP)-Adresse aufweist;
Vergleichen der DNS-Auflösungsantwort mit einer vorkonfigurierten Liste bekannter Zuordnungen von Domains zu IP-Adressen; und
Bestimmen basierend auf dem Vergleich, ob die DNS-Auflösungsantwort korrekt ist,
wobei jede IP-Adresse in der vorkonfigurierten Liste bekannter Zuordnungen von Domains zu IP-Adressen ein Bereich von IP-Adressen ist, der durch wenigstens einen Platzhalter ausgedrückt wird,
wobei die vorkonfigurierte Liste bekannter Zuordnungen von Domains zu IP-Adressen eine vorkonfigurierte Liste von Domains aufweist, die von Benutzern eines Netzwerks am häufigsten besucht werden, und
wobei die vorkonfigurierte Liste bekannter Zuordnungen von Domains zu IP-Adressen eine vorkonfigurierte Liste von Domains aufweist, die sensible Informationen hosten, auf die von Netzwerkbenutzern zugegriffen wird.



Beschreibung

Querverweis auf verwandte Offenlegungen

[0001] Diese Patentanmeldung steht mit der Patentanmeldung US 13/479,418 in Verbindung, die zeitgleich mit dieser Anmeldung eingereicht wird.

Technischer Anwendungsbereich

[0002] Die Erfindung bezieht sich im Allgemeinen auf die Identifizierung nicht vertrauenswürdiger oder manipulierter Quellen von Netzwerkinformationen. Im Besonderen bezieht sich die Erfindung auf die Identifizierung eines bösartigen DNS-Servers durch passive Überwachung.

Hintergrund

[0003] Der Domain Name Service (DNS) löst alphanumerische Domainnamen in numerische IP-Adressen auf. Dieser Dienst (bzw. Service) wird durch eine große Ansammlung von Servern bereitgestellt, die im Internet wie auch in lokalen Intranets verteilt sind. Wenn jedoch die über diesen Dienst bereitgestellten Informationen nicht von einer autorisierten Quelle stammen, sondern vielmehr von einem System eines Angreifers, das nicht korrekte Informationen liefert, oder von einer autorisierten Quelle, die manipuliert wurde, kann der Netzwerkverkehr durch einen Denial-of-Service-(DOS)-Angriff manipuliert werden oder in einem Spoofing-(Fälschungs-) oder Man-in-the-Middle-Angriff falsch weitergeleitet werden. Dies kann dazu führen, dass sensibler Datenverkehr an nicht vertrauenswürdige Systeme zugestellt wird bzw. überhaupt nicht zugestellt wird.

[0004] Eine Möglichkeit, diese Dienste zu unterlaufen, besteht darin, dass ein Angreifer einen ”Evil Twin”-WiFi-Hotspot einrichtet, der ich als vertrauenswürdiger drahtloser Zugangspunkt ausgibt und sich als Man-in-the-Middle (MITM) einrichtet, der den Netzwerkverkehr umleitet. Der MITM kann den gesamten Datenverkehr, der in das bösartige Netzwerk hineinfließt und herausgeht, untersuchen und verändern. Eine andere Möglichkeit für den Angreifer besteht darin, einen bösartigen Server einzurichten, der Netzwerkdienste kapert, indem an alle Knoten im Netzwerk eine Rundsendung abgesetzt wird, dass er online und zur Verarbeitung von DNS-Anforderungen verfügbar ist. Eine wiederum andere Möglichkeit für den Angreifer wäre es, einen vertrauenswürdigen DNS-Server zu manipulieren und ihn dazu zu veranlassen, fehlerhafte Ergebnisse zu erzeugen. In vielen Fällen wird der letzte Server, der eine Rundsendung vornimmt, von den anderen Knoten im Netzwerk als maßgeblich betrachtet.

[0005] Eine Lösung zum Erfassen solcher nicht vertrauenswürdiger oder manipulierter Quellen von Netzwerkinformationen ist die Verwendung eines DNS-Watchers (bzw. DNS-Überwachungsprogramm), der eine „Gesundheitsprüfung” (bzw. Prüfen des unversehrten Zustands) durch Polling einer vorkonfigurierten Liste vertrauenswürdiger DNS-Server ausführt, um sicherzustellen, dass sie betriebsbereit sind und korrekte Ergebnisse zurückliefern. Dieses Verfahren weist jedoch verschiedene Nachteile auf. Polling-Operationen generieren zusätzlichen, überflüssigen Netzwerkverkehr und können von einem Angreifer durch Ausspähen des Zielnetzwerks entdeckt werden. Ein Polling-Ansatz überprüft auch nur, ob die Ausführung bekannter DNS-Server korrekt ist. Aufgrund der aktiven Natur des Pollings bestimmter bekannter DNS-Server kann damit die Korrektheit von DNS-Auflösungen nicht geprüft werden, die von anderen als den bekannten abgefragten Hosts zurückgegeben werden. Da bösartige DNS-Provider nicht vorab bekannt sind, würden sie von einer Polling-Lösung nicht entdeckt werden.

Kurzbeschreibung

[0006] Im Allgemeinen stellen Aspekte der vorliegenden Erfindung eine passive Überwachungslösung zur Identifizierung eines bösartigen DNS-Servers in einem Netzwerk bereit, die keinen zusätzlichen Netzwerkverkehr generiert und die in der Lage ist, DNS-Auflösungen zu überwachen, die sowohl von bekannten als auch nicht bekannten DNS-Servern bereitgestellt werden.

[0007] Ein erster Aspekt der Offenlegung stellt ein Verfahren zur Identifizierung eines bösartigen Domain-Name-Service-(DNS)-Servers bereit. Das Verfahren weist auf: passives Überwachen von Datenverkehr in einem Netzwerk; Identifizieren einer DNS-Auflösungsantwort im Datenverkehr im Netzwerk, wobei die DNS-Auflösungsantwort eine Zuordnung einer Domain zu einer Internetprotokoll(IP)-Adresse aufweist; Vergleichen der DNS-Auflösungsantwort mit einer vorkonfigurierten Liste bekannter Zuordnungen von Domains zu IP-Adressen; und Bestimmen, ob die DNS-Auflösungsantwort basierend auf dem Vergleich korrekt ist.

[0008] Ein zweiter Aspekt der Offenlegung stellt ein System zur Identifizierung eines bösartigen Domain-Name-Service-(DNS)-Servers bereit. Das System weist auf: eine Überwachungskomponente zum passiven Überwachen von Datenverkehr in einem Netzwerk; eine Identifizierungskomponente zum Identifizieren einer DNS-Auflösungsantwort im Datenverkehr im Netzwerk, wobei die DNS-Auflösungsantwort eine Zuordnung einer Domain zu einer Internetprotokoll(IP)-Adresse aufweist; eine Vergleichskomponente zum Vergleichen der DNS-Auflösungsantwort mit einer vorkonfigurierten Liste bekannter Zuordnungen von Domains zu IP-Adressen; und eine Bestimmungskomponente zum Bestimmen, ob die DNS-

Auflösungsantwort basierend auf dem Vergleich korrekt ist.

[0009] Ein dritter Aspekt der Offenlegung stellt ein in einem computerlesbaren Speichermedium ausgeführtes Computerprogrammprodukt bereit, bei dessen Ausführung durch eine Computingvorrichtung das Computersystem dazu veranlasst wird, ein Verfahren zur Identifizierung eines bösartigen Domain-Name-Service-(DNS)-Server zu implementieren. Das Verfahren weist auf: passives Überwachen von Datenverkehr in einem Netzwerk; Identifizieren einer DNS-Auflösungsantwort im Datenverkehr im Netzwerk, wobei die DNS-Auflösungsantwort eine Zuordnung einer Domain zu einer Internetprotokoll (IP)-Adresse aufweist; Vergleichen der DNS-Auflösungsantwort mit einer vorkonfigurierten Liste bekannter Zuordnungen von Domains zu IP-Adressen; und Bestimmen, ob die DNS-Auflösungsantwort basierend auf dem Vergleich korrekt ist.

[0010] Diese und andere Aspekte, Vorteile und herausragende Merkmale der Erfindung werden aus der folgenden Detailbeschreibung ersichtlich, die in Verbindung mit den Zeichnungen im Anhang, wo in den Zeichnungen ähnliche Teile durch ähnliche Bezugszeichen bezeichnet werden, Ausführungsformen der Erfindung offenlegt.

Kurzbeschreibung der Zeichnungen

[0011] **Fig.** 1 zeigt ein Datenverarbeitungssystem, das für die Implementierung einer Ausführungsform der Erfindung geeignet ist.

[0012] **Fig.** 2 zeigt ein schematisches Datenflussdiagramm, das die Überwachung eines Netzwerks gemäß einer Ausführungsform der Erfindung veranschaulicht.

[0013] **Fig.** 3 zeigt ein schematisches Datenflussdiagramm, das die Identifizierung eines bösartigen DNS-Servers gemäß einer Ausführungsform der Erfindung veranschaulicht.

[0014] **Fig.** 4 zeigt eine vorkonfigurierte DNS-Auflösungstabelle gemäß einer Ausführungsform der Erfindung.

[0015] **Fig.** 5 zeigt ein Flussdiagramm eines Verfahrens zur Identifizierung eines bösartigen DNS-Servers gemäß einer Ausführungsform der Erfindung.

[0016] Die Zeichnungen müssen nicht skaliert werden. Die Zeichnungen stellen nur Schemadarstellungen dar, die nicht dazu gedacht sind, spezielle Parameter der Erfindung abzubilden. Die Zeichnungen sind dazu gedacht, nur typische Ausführungsformen der Erfindung darzustellen und sollten daher nicht als Einschränkung des Umfangs der Erfindung betrachtet werden. In den Zeichnungen stellen ähnliche Referenznummern ähnliche Elemente dar.

Detaillierte Beschreibung der Erfindung

[0017] Wie oben ausgeführt, stellen Aspekte der vorliegenden Erfindung eine Lösung zum Erfassen des Vorhandenseins eines bösartigen DNS-Servers über die Verwendung eines Monitors bereit, der den Fluss des Datenverkehrs zwischen den Knoten in einem Netzwerk passiv beobachtet und in dem Netzwerk nach gefälschtem DNS-Datenverkehr sucht. In einigen Ausführungsformen kann das Netzwerk ein lokales Internet sein und in anderen kann das Netzwerk das Internet sein.

[0018] Es wird nun auf die Zeichnungen Bezug genommen. **Fig.** 1 zeigt einen veranschaulichenden Monitor **100** zum Erfassen des Vorhandenseins eines bösartigen DNS-Servers **215**, der im Netzwerk **200** vorhanden sein kann. In diesem Umfang weist der Monitor **101** ein Computersystem **102** auf, das einen wie in diesem Dokument beschriebenen Prozess durchführen kann, um eine ungültige DNS-Auflösungsantwort von einem bösartigen DNS-Server **215** zu identifizieren. Im Besonderen wird ein Computersystem **102** mit einer Computingvorrichtung **104** dargestellt, die ein Identifizierungsprogramm **140** für einen bösartigen DNS-Server aufweist, durch das die Computingvorrichtung **104** funktionsfähig wird, einen bösartigen DNS-Server **215** zu identifizieren, indem ein in diesem Dokument beschriebener Prozess durchgeführt wird.

[0019] Die Computingvorrichtung **104** ist dargestellt mit einer Verarbeitungseinheit **106** (z. B. einen oder mehreren Prozessoren), einem Speicher (Memory) **110**, einem Speichersystem (Storage System) **118** (z. B, einer Speicherhierarchie), einer Eingabe-/Ausgabe (Input/Output, I/O)-Schnittstellenkomponente **114** (z. B. eine oder mehrere I/O-Schnittstellen und/oder -vorrichtungen) und einen Kommunikations-Pathway **112**. Im Allgemeinen führt die Verarbeitungseinheit **106** Programmcode aus, wie das Identifizierungsprogramm **140** für einen bösartigen DNS-Server, das wenigstens teilweise fest im Speicher **110** vorliegt. In diesem Umfang kann die Verarbeitungseinheit **106** eine einzelne Verarbeitungseinheit aufweisen oder über eine oder mehrere Verarbeitungseinheit an einem oder mehreren Standorten verteilt sein.

[0020] Der Speicher **110** kann auch lokalen Speicher aufweisen, der bei der konkreten Ausführung des Programmcodes genutzt wird, Massenspeicher (Speicher **118**) und/oder Cachespeicher (nicht dargestellt), die einen temporären Speicher für wenigsten einen Teil des Programmcode bereitstellen, damit Code bei der Ausführung nicht so oft aus dem Massenspeicher **118** abgerufen werden muss. So kann der Speicher **110** jeden bekannten Typ von Daten-

speichern und/oder Übertragungsmedien aufweisen, einschließlich magnetischer Medien, optischer Medien, Direktzugriffsspeicher (Random Access Memory, RAM), Festspeicher (Read-only Memory, ROM), eines Datencaches, eines Datenobjekts usw. Darüber hinaus kann der Speicher **110**, ähnlich wie die Verarbeitungseinheit **116**, sich an einem einzigen physischen Standort befinden, einen oder mehrere Typen von Datenspeichern aufweisen oder über eine Vielzahl physischer Systeme in verschiedenen Formen verteilt sein.

[0021] Bei der Ausführung des Programmcodes kann die Verarbeitungskomponente **106** Daten verarbeiten, was zum Lesen und/oder Schreiben umgewandelter Daten aus/in den Speicher **110** und/oder der I/O-Komponente **114** zur weiteren Verarbeitung führen kann. Der Pathway **112** stellt eine direkte oder indirekte Kommunikationsverbindung zwischen jeder der Komponenten im Computersystem **102** bereit. Die I/O-Schnittstellenkomponente **114** kann einen oder mehrere für menschliche Benutzer konzipierte I/O-Vorrichtungen aufweisen, die einem menschlichen Benutzer **120** die Interaktion mit dem Computersystem **102** und/oder einen oder mehreren Kommunikationsvorrichtungen ermöglichen, um einem Systembenutzer **120** die Kommunikation mit dem Computersystem **102** über jede beliebige Art von Kommunikationsverbindung zu ermöglichen.

[0022] In diesem Umfang kann ein Identifizierungsprogramm **140** für einen bösartigen DNS-Server eine Gruppe von Schnittstellen (z. B. grafische Benutzeroberfläche(n), Anwendungsprogrammschnittstelle und/oder Ähnliches) verwalten, mit denen menschliche und/oder Systembenutzer **120** mit dem Identifizierungsprogramm **140** für einen bösartigen DNS-Server interagieren können. Weiterhin kann das Identifizierungsprogramm **140** für einen bösartigen DNS-Server die Daten, wie die in der Tab. **220** (**Fig.** 2–**Fig.** 4) gespeicherten Daten, unter Verwendung jeder beliebigen Lösung verwalten (z. B. speichern, abrufen, erstellen, bearbeiten, organisieren, darstellen usw.).

[0023] In jeden Fall kann ein Computersystem **102** eine oder mehrere allgemeine Computing-Fertigungsprodukte **104** (wie Computingvorrichtungen) aufweisen, die in der Lage sind, darauf installierten Programmcode, wie das Identifizierungsprogramm **140** für einen bösartigen DNS-Server, auszuführen. Wie in diesem Dokument verwendet, versteht es sich, dass „Programmcode" eine beliebige Zusammenstellung von Anweisungen in einer beliebigen Sprache, einem beliebigen Code oder einer beliebigen Notation bedeutet, die/der eine Computingvorrichtung mit einer Informationsverarbeitungsfähigkeit veranlasst, eine bestimmte Aktion entweder direkt oder nach einer beliebigen Kombination des Folgenden durchzuführen: (a) Konvertierung in eine andere Sprache, einen anderen Code oder eine andere Notation; (b) Reproduktion in einer anderen materiellen Form; und/oder (c) Dekomprimierung. In diesem Umfang kann ein Identifizierungsprogramm **140** für einen bösartigen DNS-Server als eine beliebige Kombination von Systemsoftware und/oder Anwendungssoftware ausgeführt werden. In jeden Fall besteht die technische Wirkung des Computersystems **102** darin, Verarbeitungsanweisungen für die Computingvorrichtung **104** bereitzustellen, um einen bösartigen DNS-Server zu identifizieren.

[0024] Weiterhin kann ein Identifizierungsprogramm **140** für einen bösartigen DNS-Server mit einer Gruppe von Modulen **142**–**150** implementiert werden. In diesem Fall kann ein Modul **142**–**150** dem Computersystem **102** ermöglichen, eine von dem Identifizierungsprogramm **140** des bösartigen DNS-Servers verwendete Gruppe von Aufgaben durchzuführen und kann eigenständig, getrennt von anderen Bereichen des Identifizierungsprogramms **140** für einen bösartigen DNS-Server entwickelt und/oder implementiert werden. Gemäß der Verwendung in diesem Dokument bedeutet der Begriff „Komponente" eine beliebige Hardwarekonfiguration mit oder ohne Software, die die in Verbindung damit beschriebene Funktionalität unter Verwendung einer beliebigen Lösung implementiert, während der Begriff „Modul" für Programmcode steht, der einem Computersystem **102** die Implementierung der in Verbindung damit beschriebenen Aktionen unter Verwendung einer beliebigen Lösung ermöglicht. Wenn ein Modul in einem Speicher **110** eines Computersystems **102**, das eine Verarbeitungskomponente **106** aufweist, fest vorliegt, ist es ein wesentlicher Bestandteil einer Komponente, die die Aktionen implementiert. Unabhängig davon versteht es sich, dass zwei oder mehr Komponenten, Module und/oder Systeme einige Teile/alle Teile der zugehörigen Hardware und/oder Software gemeinsam verwenden können. Weiterhin versteht es sich, dass einige Teile der hier erörterten Funktionalität nicht als Bestandteil des Computersystems **102** implementiert werden können oder dass weitere Funktionalität als Teil des Computersystems **102** enthalten sein kann.

[0025] Wenn das Computersystem **102** mehrere Computingvorrichtungen **104** aufweist, kann jede Computingvorrichtung **104** nur einen Bereich des Identifizierungsprogramms **140** eines bösartigen DNS-Servers darauf fest vorliegend haben (z. B. ein oder mehrere Module **142**–**150**). Es versteht sich aber, dass das Computersystem **102** und ein Identifizierungsprogramm **140** für einen bösartigen DNS-Server nur für verschiedene mögliche gleichwertige Computersysteme stehen, die einen in diesem Dokument beschriebenen Prozess ausführen können. In diesem Umfang kann die vom Computersystem **102** und dem Identifizierungsprogramm **140** für einen bösartigen DNS-Server bereitgestellte Funktionalität

in anderen Ausführungsformen wenigstens teilweise durch eine oder mehrere Computingvorrichtungen implementiert werden, die eine beliebige Kombination allgemeiner und/oder Spezialhardware mit oder ohne Programmcode aufweisen. In jeder Ausführungsform kann die Hardware und der Programmcode, falls enthalten, jeweils mit standardmäßigen Engineering- und Programmiertechniken erstellt werden.

[0026] Wenn das Computersystem **102** mehrere Computingvorrichtungen **104** aufweist, können die Computingvorrichtungen über jede Art von Kommunikationsverbindung kommunizieren. Weiterhin kann das Computersystem **102** bei der Durchführung eines in diesem Dokument beschriebenen Prozesses mit einem oder mehreren Computersystemen unter Verwendung einer beliebigen Art von Kommunikationsverbindung kommunizieren. In jedem Fall kann die Kommunikationsverbindung eine beliebige Kombination von verschiedenen Arten von kabelgebundenen und/oder drahtlosen Verbindungen aufweisen; eine beliebige Kombination von einem oder mehreren Typen von Netzwerken aufweisen; und/oder eine beliebige Kombination von verschiedenen Arten von Übertragungstechniken und -protokollen nutzen.

[0027] Wie in dem vorliegenden Dokument erörtert, ermöglicht das Identifizierungsprogramm **140** für einen bösartigen DNS-Server dem Computersystem **102**, eine Identifizierung eines bösartigen DNS-Servers zu implementieren. In diesem Umfang wird ein Identifizierungsprogramm **140** für einen bösartigen DNS-Server einschließlich eines Überwachungsmoduls **142**, eines Identifizierungsmoduls **144**, eines Vergleichsmoduls **146**, eines Bestimmungsmoduls **148** und eines Alarmmoduls **150** dargestellt.

[0028] Im Folgenden wird nun auf **Fig.** 2–**Fig.** 3 Bezug genommen, wo die Netzwerkumgebung **200**, in der der Monitor **100** verwendet werden kann, dargestellt wird. Wie dargestellt, kann ein Netzwerk **200** einen Anforderer (Requester) **205** enthalten, der eine von einem Benutzer oder einem Server betriebene Client-Workstation sein kann. Weitere Anforderer **205** können im Netzwerk **200** enthalten sein, sie wurden aber aus Gründen der Einfachheit in der Darstellung des Netzwerks **200** in den **Fig.** 2–**Fig.** 3 weggelassen. Der Anforderer **205** kann eine DNS-Auflösungsanforderung **201** zur Auflösung eines alphanumerischen Domainnamens eines bestimmten Hosts in eine numerische IP-Adresse senden.

[0029] Wie in **Fig.** 2 dargestellt, wird unter normalen Betriebsbedingungen, bei denen im Netzwerk **200** kein Angreifer vorhanden ist, die DNS-Auflösungsanforderung **201** empfangen und vom autorisierten DNS-Server **210** verarbeitet, der eine DNS-Auflösungsantwort **202** sendet. In diesem Fall kann die DNS-Auflösungsantwort **202** eine gültige und exakte Zuordnung des Domainnamens zur IP-Adresse enthalten.

[0030] In anderen Fällen, wie in **Fig.** 3 dargestellt, kann ein bösartiger DNS-Server **215** eines Angreifers im Netzwerk **200** zum Zweck der Nachahmung eines anderen Computingsystems vorhanden sein. In diesem Fall wird von einem bösartigen DNS-Server **215** eine DNS-Auflösungsanforderung **201** empfangen und verarbeitet und die DNS-Auflösungsantwort **202** wird vom bösartigen DNS-Server **215** bereitgestellt. Eine solche DNS-Auflösungsantwort **202** kann eine nicht korrekte Zuordnung des Domainnamens zur IP-Adresse aufweisen, was entweder zu einer falschen Weiterleitung des Netzwerkverkehrs in einem Spoofing-Angriff führt, bei dem sensibler Datenverkehr an ein nicht vertrauenswürdiges System geliefert wird, oder der Netzwerkverkehr in einem Denial-of-Service(DOS)-Angriff behindert wird.

[0031] In beiden Fällen ist der Monitor **100** an einem strategischen Punkt im Netzwerk **200** positioniert, sodass der Monitor **100** den Fluss des Netzwerkverkehrs zwischen den Knoten im Netzwerk **200** beobachten kann. Wie oben mit Bezugnahme auf **Fig.** 1 erörtert, weist der Monitor **100** die Module **142**–**150** auf, die bei der Ausführung durch ein Computersystem **102** die passive Überwachung des Datenverkehrs im Netzwerk **200** durchführen, darunter unter anderem des Netzwerkverkehrs, der DNS-Auflösungsanforder- ung **201** und der DNS-Auflösungsantwort **202**.

[0032] Es wird gleichzeitig auf die **Fig.** 1–**Fig.** 3 Bezug genommen, wobei das Überwachungsmodul **142** als Bestandteil des Monitors **100** die Überwachung **143** des Datenverkehrs im Netzwerk **200** durchführt, darunter die DNS-Auflösungsanforderungen **201** und die DNS-Auflösungsantworten **202**. Die Identifizierungskomponente **144** kann in dem im Netzwerk **200** überwachten Datenverkehr eine DNS-Auflösungsantwort **202** identifizieren. Wie oben erwähnt, weist eine DNS-Auflösungsantwort **202** eine Zuordnung eines Domainnamens **225** zu einer IP-Adresse **230** als Reaktion auf eine vom Anforderer **205** gesendete DNS-Auflösungsanforderung **201** auf.

[0033] Sobald eine DNS-Auflösungsantwort **202** identifiziert ist, kann ein Vergleichsmodul **146** einen Vergleich der DNS-Auflösungsantwort **202** vornehmen, wobei die bekannten Zuordnungen in einer vorkonfigurierten Liste bekannter Zuordnungen von Domainnamen zu IP-Adressen, die in einer bekannten DNS-Auflösungstabelle **220** enthaltenen sind, gespeichert sind. Es ist bekannt, dass die in Tabelle **220** enthaltenen Zuordnungen von Domainnamen zu IP-Adressen gültig sind. Wie in **Fig.** 4 dargestellt, kann die in Tabelle **220** gespeicherte IP-Adresse **230** als eine spezielle IP-Adresse ausgedrückt werden, wie yyy.yyy.yyy.yyy, die IP-Adresse der Domain my-

bank.com. In anderen Ausführungsformen können die in der Tabelle **200** gespeicherten IP-Adressen **230** als Bereich von IP-Adressen unter Verwendung von wenigstens einem Platzhalter ausgedrückt werden. Ein Bereich von IP-Adressen kann breit gefächert sein, darunter verschiedene Platzhalter wie zum Beispiel xxx.*.*.*, der IP-Adressbereich für die Domain company.com. In anderen Ausführungsformen kann der Bereich von IP-Adressen enger gefasst sein, zum Beispiel mit nur einem Platzhalter, wie zzz.zzz.zzz.1??, der IP-Adressbereich für die Domain email.org.

[0034] Gemäß Ausführungsformen der Erfindung muss die in der Tabelle **220** gespeicherte Liste der zugewiesenen Domainnamen **225** und IP-Adressen **230** keine erschöpfende Liste von Domains sein, auf die ein Benutzer von Netzwerk **200** zugreifen kann oder für die ein Anforderer **205** DNS-Auflösungen anfordern kann. Stattdessen kann eine ausgewählte Anzahl an Hosts in der Tabelle **220** als repräsentative Stichprobe enthalten sein. In einigen Ausführungsformen kann die Tabelle **220** eine vorkonfigurierte Liste von Domains und deren zugehörige IP-Adressen enthalten, deren Auswahl zur Aufnahme in Tabelle **220** auf der Domain basiert, die besonders sensible Informationen, auf die die Netzwerkbenutzer zugreifen, hostet. In anderen Ausführungsformen kann die Tabelle **220** eine vorkonfigurierte Liste von Domains und deren zugehörige IP-Adressen aufweisen, deren Auswahl zur Aufnahme in Tabelle **220** auf einer hohen Anzahl von Besuchen durch Benutzer des Netzwerks **200** und daher auf einer hohen Wahrscheinlichkeit eines großen zu überwachenden Stichprobenpools von DNS-Auflösungsanforderungen und -antworten basiert.

[0035] Es wird wieder auf **Fig.** 1–**Fig.** 3 Bezug genommen. Das Bestimmungsmodul **148** führt eine Bestimmung durch, ob die DNS-Auflösungsantwort **202** eine korrekte und gültige Zuordnung der IP-Adresse zum Domainnamen enthält. Diese Bestimmung basiert auf dem vom Vergleichsmodul **146** durchgeführten Vergleich. Wenn die Zuordnung in der DNS-Auflösungsantwort **202** der Zuordnung für den in der Tabelle **220** gespeicherten entsprechenden Domainnamen entspricht, wird die DNS-Auflösungsantwort **202** als korrekt bestimmt. Dies gibt an, dass die DNS-Auflösungsantwort **202** zu dem autorisierten DNS-Server **210** gesendet wurde (**Fig.** 2). Wenn die Zuordnung in der DNS-Auflösungsantwort **202** nicht der Zuordnung für den in der Tabelle **220** gespeicherten entsprechenden Domainnamen entspricht, wird die DNS-Auflösungsantwort **202** als nicht korrekt bestimmt. Es gibt an, dass die DNS-Auflösungsantwort **202** an einen bösartigen DNS-Server **215** gesendet wurde (**Fig.** 3), und kann auf das Auftreten eines Spoofing- oder DOS-Angriffs hinweisen. In diesem Fall sendet das Alarmmodul **150** einen Alarm **240**, um den Anforderer **205** über den gefälschten DNS-Datenverkehr zu informieren. In verschiedenen Ausführungsformen kann der Alarm **240** die Form einer Nachricht (E-Mail, SMS usw.), eines Logeintrags oder einer anderen Form von Benachrichtigung über ein Sicherheitsereignis annehmen, das das verdächtige Verhalten dokumentiert und die Aufmerksamkeit darauf lenkt.

[0036] Das obige Verfahren wird in einem Flussdiagramm in **Fig.** 5 dargestellt. Wie oben beschrieben, überwacht ein Monitor passiv den Datenverkehr in einem Netzwerk. Über dieses Netzwerk fordert eine anfordernde Workstation eine DNS-Auflösung einer bestimmten Domain an.

[0037] Eine DNS-Auflösungsantwort wird von einem DNS-Server an den Anforderer über das Netzwerk zurückgegeben. Die DNS-Auflösungsantwort wird vom Monitor aus dem überwachten Netzwerkverkehr identifiziert. Nach der Identifizierung wird die Zuordnung einer IP-Adresse zu einer Domain, die in der DNS-Auflösungsantwort enthaltenen ist, mit einer vorkonfigurierten Liste bekannter Zuordnungen von IP-Adressen zu Domains verglichen. Wenn weder die Domain noch die IP-Adresse in der DNS-Auflösungsantwort in der vorkonfigurierten Liste bekannter Zuordnungen von IP-Adressen zu Domains erscheint, kehrt der Monitor einfach zur Überwachung des Netzwerks zurück.

[0038] Wenn entweder die Domain oder die IP-Adresse in der DNS-Auflösungsantwort in der vorkonfigurierten Liste bekannter Zuordnungen von IP-Adressen zu Domains erscheint, wird die in der DNS-Auflösungsanforderung enthaltene Zuordnung mit der entsprechenden Zuordnung in der vorkonfigurierten Liste bekannter Zuordnungen von IP-Adressen zu Domains verglichen. Wenn die Zuordnung übereinstimmt, d. h. sowohl die IP-Adresse und die entsprechende Domain in der DNS-Auflösungsantwort und der vorkonfigurierten Liste bekannter Zuordnungen von IP-Adressen zu Domains identisch sind, dann kann bestimmt werden, dass die DNS-Auflösungsantwort korrekt ist und der DNS-Server, der sie gesendet hat, autorisiert ist. Wenn jedoch die Zuordnung nicht übereinstimmt, d. h. die Domains unterschiedlichen IP-Adressen in der DNS-Auflösungsantwort und der vorkonfigurierten Liste bekannter Zuordnung von IP-Adressen zu Domains entspricht (oder die IP-Adresse entspricht unterschiedlichen Domains in der DNS-Auflösungsantwort und der vorkonfigurierten Liste bekannter Zuordnungen von IP-Adressen zu Domains), dann kann bestimmt werden, dass die DNS-Auflösungsantwort ungültig ist. In diesem Fall kann daraus geschlossen werden, dass der DNS-Server, der sie gesendet hat, nicht autorisiert ist und ein bösartiger DNS-Server sein kann. In diesem Fall wird ein Alarm ausgelöst, der den Anforderer über das Sicherheitsrisiko benachrichtigt.

[0039] Wenngleich die Erfindung in diesem Dokument als ein Verfahren und System zur Identifizierung eines bösartigen DNS-Servers dargestellt und beschrieben wird, versteht es sich, dass Aspekte der Erfindung weiterhin verschiedene alternative Ausführungsformen vorsehen können. Zum Beispiel sieht die Erfindung in einer Ausführungsform ein Computerprogramm vor, das auf wenigstens einem computerlesbaren Medium fest vorliegt, das bei der Ausführung einem Computersystem ermöglicht, die Identifizierung eines bösartigen DNS-Servers zu implementieren. In diesem Umfang weist das computerlesbare Medium Programmcode auf, wie das Identifizierungsprogramm **140** für einen bösartigen DNS-Server (**Fig.** 1), der einige oder alle der in diesem Dokument beschriebenen Prozesse implementiert. Es versteht sich, dass der Begriff „computerlesbares Medium" ein oder mehrere eines beliebigen Typs eines materiellen Ausdruckmediums aufweist, dass nicht bekannt oder in Zukunft entwickelt wird, von dem ein Exemplar des Programmcode erhalten, wiedergegeben oder anderweitig durch eine Computingvorrichtung kommuniziert werden kann. Zum Beispiel kann das computerlesbare Medium aufweisen: eine oder mehrere tragbare Speicherfertigungsprodukte; ein oder mehrere Speicherkomponenten (Memory/Storage) einer Computingvorrichtung; Papier und/oder Ähnliches.

[0040] In einer anderen Ausführungsform stellt die Erfindung ein Verfahren bereit, das ein Exemplar von Programmcode bereitstellt, wie das Identifizierungsprogramm **140** für einen bösartigen DNS-Server (**Fig.** 1), das einige oder alle der in diesem Dokument beschriebenen Prozesse implementiert. In diesem Fall kann ein Computersystem ein Exemplar von Programmcode verarbeiten, der einen Teil oder den gesamten des in diesem Dokument beschriebenen Prozesses implementiert, um für den Empfang an einem zweiten entfernten Standort eine Gruppe von Datensignalen zu generieren und zu übertragen, die einen oder mehrere seiner Eigenschaften dergestalt festgelegt und/oder geändert haben, um ein Exemplar des Programmcodes in der Gruppe von Datensignalen zu kodieren. Ebenso stellt eine Ausführungsform der Erfindung ein Verfahren zum Erfassen eines Exemplars von Programmcode bereit, der einen Teil oder den gesamten des in diesem Dokument beschriebenen Prozesses implementiert, was ein Computersystem aufweist, dass die in diesem Dokument beschriebene Gruppe von Datensignale empfängt und die Gruppe von Datensignalen in ein Exemplar des Computerprogramms übersetzt, das wenigstens auf einem computerlesbaren Medium fest vorliegt. In jedem Fall kann die Gruppe von Datensignalen mit jeder beliebigen Art von Kommunikationsverbindung übertragenen/empfangen werden.

[0041] In wiederum einer anderen Ausführungsform stellt die Erfindung ein Verfahren zum Generieren eines Systems zur Identifizierung eines bösartigen DNS-Servers bereit. In diesem Fall kann ein Computersystem, wie das Computersystem **102** (**Fig.** 1), erhalten werden (z. B. erstellt, verwaltet, verfügbar gemacht werden usw.) und eine oder mehrere Komponenten zum Durchführen eines in diesem Dokument beschriebenen Prozesses können erhalten (z. B. erstellt, erworben, verwendet, geändert usw.) und auf dem Computersystem bereitgestellt werden. In diesem Umfang kann die Bereitstellung (Deployment) eines oder mehrere aufweisen von: (1) Installation von Programmcode auf einer Computingvorrichtung; (2) Hinzufügen von einer oder mehreren Computing- und/oder I/O-Vorrichtungen zu dem Computersystem; (3) Aufnahme und/oder Modifikation des Computersystems, um die Durchführung eines in diesem Dokument beschriebenen Prozesses zu ermöglichen; und/oder Ähnliches.

[0042] Wie in diesem Dokument verwendet, bezeichnen die Begriffe „erstes", „zweites" und Ähnliche nicht eine Reihenfolge, Menge oder Bedeutung, sondern werden nur zur Unterscheidung eines Elements von einem anderen verwendet, und die Begriffe „ein" oder „eine" bezeichnen hier keine Mengenbeschränkung, sondern geben stattdessen das Vorhandensein von wenigstens einem der referenzierten Elemente an. Der in Verbindung mit einer Mengenangabe verwendete Modifizierer „etwa" schließt den angegebenen Wert mit ein und hat die vom Kontext vorgegebene Bedeutung (enthält zum Beispiel den Fehlergrad, der der Messung einer bestimmten Menge zugeordnet ist). Das Suffix „(en)" ist gemäß der Verwendungen in diesem Dokument dazu gedacht, sowohl die Singular- wie auch die Pluralform des zu modifizierenden Begriffs zu beinhalten, wodurch ein oder mehrere Vorkommen des Begriffes (wie zum Beispiel Verarbeitungseinheit(en) ein oder mehrere Bearbeitungseinheiten beinhaltet) beinhalten. Die in diesem Dokument offengelegten Bereiche sind inkludierend und unabhängig kombinierbar (z. B. Bereiche von „bis zu etwa drei Platzhaltern" oder im Besonderen beinhaltet „etwa ein Platzhalter bis etwa drei Platzhalter" die Endpunkte und alle Zwischenwerte der Bereiche von „etwa ein Platzhalter bis etwa zwei Platzhalter" usw.).

[0043] Die Beschreibungen der verschiedenen Ausführungsformen der vorliegenden Erfindung wurden für Veranschaulichungszwecke dargestellt, ist jedoch nicht dazu gedacht, als erschöpfend oder auf die offengelegten Ausführungsformen beschränkt zu sein. Für Fachleute werden viele Modifikationen und Variationen ersichtlich sein, ohne dabei vom Umfang und Geist der beschriebenen Ausführungsformen abzuweichen. Die hier verwendete Terminologie wurde gewählt, um die Prinzipien der Ausführungsformen, der praktischen Anwendung oder der technischen Verbesserung gegenüber im Markt erhältlichen Technologien am besten zu erklären, oder um anderen

Fachleuten das Verständnis der hier offengelegten Ausführungsformen zu ermöglichen.

Patentansprüche

1. Ein Verfahren zum Identifizieren eines bösartigen Domain Name Service(DNS)-Servers, wobei das Verfahren aufweist:
passives Überwachen von Datenverkehr in einem Netzwerk;
Identifizieren einer DNS-Auflösungsantwort im Datenverkehr im Netzwerk, wobei die DNS-Auflösungsantwort eine Zuordnung einer Domain zu einer Internetprotokoll(IP)-Adresse aufweist;
Vergleichen der DNS-Auflösungsantwort mit einer vorkonfigurierten Liste bekannter Zuordnungen von Domains zu IP-Adressen; und
Bestimmen basierend auf dem Vergleich, ob die DNS-Auflösungsantwort korrekt ist,
wobei jede IP-Adresse in der vorkonfigurierten Liste bekannter Zuordnungen von Domains zu IP-Adressen ein Bereich von IP-Adressen ist, der durch wenigstens einen Platzhalter ausgedrückt wird,
wobei die vorkonfigurierte Liste bekannter Zuordnungen von Domains zu IP-Adressen eine vorkonfigurierte Liste von Domains aufweist, die von Benutzern eines Netzwerks am häufigsten besucht werden, und
wobei die vorkonfigurierte Liste bekannter Zuordnungen von Domains zu IP-Adressen eine vorkonfigurierte Liste von Domains aufweist, die sensible Informationen hosten, auf die von Netzwerkbenutzern zugegriffen wird.

2. Das Verfahren nach Anspruch 1, das weiterhin ein Senden eines Alarms in dem Fall aufweist, in dem die DNS-Auflösungsantwort als nicht korrekt bestimmt wird.

3. Das Verfahren nach Anspruch 2, wobei der Alarm wenigstens eines aufweist von einer E-Mail-Nachricht, einer SMS-Nachricht, einem Logeintrag oder einer Benachrichtigung über einen Sicherheitsvorfall.

4. Das Verfahren nach Anspruch 1, wobei das Netzwerk ein Internet aufweist.

5. Ein System zum Identifizieren eines bösartigen Domain Name Service(DNS)-Servers, wobei das System aufweist:
eine Überwachungskomponente zur passiven Überwachung von Datenverkehr in einem Netzwerk;
eine Identifizierungskomponente zum Identifizieren einer DNS-Auflösungsantwort im Datenverkehr im Netzwerk, wobei die DNS-Auflösungsantwort eine Zuordnung einer Domain zu einer Internetprotokoll (IP)-Adresse aufweist;
eine Vergleichskomponente zum Vergleichen der DNS-Auflösungsantwort mit einer vorkonfigurierten Liste bekannter Zuordnungen von Domains zu IP-Adressen; und
eine Bestimmungskomponente zum Bestimmen basierend auf dem Vergleich, ob die DNS-Auflösungsantwort korrekt ist,
wobei jede IP-Adresse in der vorkonfigurierten Liste bekannter Zuordnungen von Domains zu IP-Adressen ein Bereich von IP-Adressen ist, der durch wenigstens einen Platzhalter ausgedrückt wird,
wobei die vorkonfigurierte Liste bekannter Zuordnungen von Domains zu IP-Adressen eine vorkonfigurierte Liste von Domains aufweist, die von Benutzern eines Netzwerks am häufigsten besucht werden, und
wobei die vorkonfigurierte Liste bekannter Zuordnungen von Domains zu IP-Adressen eine vorkonfigurierte Liste von Domains aufweist, die sensible Informationen hosten, auf die von Netzwerkbenutzern zugegriffen wird.

6. Das System nach Anspruch 5, das weiterhin eine Alarmkomponente zum Senden eines Alarms in dem Fall aufweist, wenn die DNS-Auflösungsantwort als nicht korrekt bestimmt wird.

7. Das System nach Anspruch 5, wobei die Alarmkomponente wenigstens eines aufweist von einer E-Mail-Nachricht, einer SMS-Nachricht, einem Logeintrag oder einer Benachrichtigung über einen Sicherheitsvorfall.

8. Das System nach Anspruch 5, wobei das Netzwerk ein Internet aufweist.

9. Ein in einem computerlesbaren Speichermedium ausgeführtes Computerprogrammprodukt, das bei dessen Ausführung durch eine Computingvorrichtung das Computersystem dazu veranlasst, ein Verfahren zur Identifizierung eines bösartigen Domain Name Service(DNS)-Servers zu implementieren, wobei das Verfahren aufweist:
passives Überwachen von Datenverkehr in einem Netzwerk;
Identifizieren einer DNS-Auflösungsantwort im Datenverkehr im Netzwerk, wobei die DNS-Auflösungsantwort eine Zuordnung einer Domain zu einer Internetprotokoll(IP)-Adresse aufweist;
Vergleichen der DNS-Auflösungsantwort mit einer vorkonfigurierten Liste bekannter Zuordnungen von Domains zu IP-Adressen; und
Bestimmen basierend auf dem Vergleich, ob die DNS-Auflösungsantwort korrekt ist,
wobei jede IP-Adresse in der vorkonfigurierten Liste bekannter Zuordnungen von Domains zu IP-Adressen ein Bereich von IP-Adressen ist, der durch wenigstens einen Platzhalter ausgedrückt wird,
wobei die vorkonfigurierte Liste bekannter Zuordnungen von Domains zu IP-Adressen eine vorkonfigurierte Liste von Domains aufweist, die von Benutzern eines Netzwerks am häufigsten besucht werden, und

wobei die vorkonfigurierte Liste bekannter Zuordnungen von Domains zu IP-Adressen eine vorkonfigurierte Liste von Domains aufweist, die sensible Informationen hosten, auf die von Netzwerkbenutzern zugegriffen wird.

10. Das Computerprogrammprodukt nach Anspruch 9, wobei das Verfahren weiterhin das Senden eines Alarms in dem Fall aufweist, in dem die DNS-Auflösungsantwort als nicht korrekt bestimmt wird.

11. Das Computerprogrammprodukt nach Anspruch 9, wobei das Netzwerk ein Intranet aufweist.

Es folgen 5 Seiten Zeichnungen

Anhängende Zeichnungen

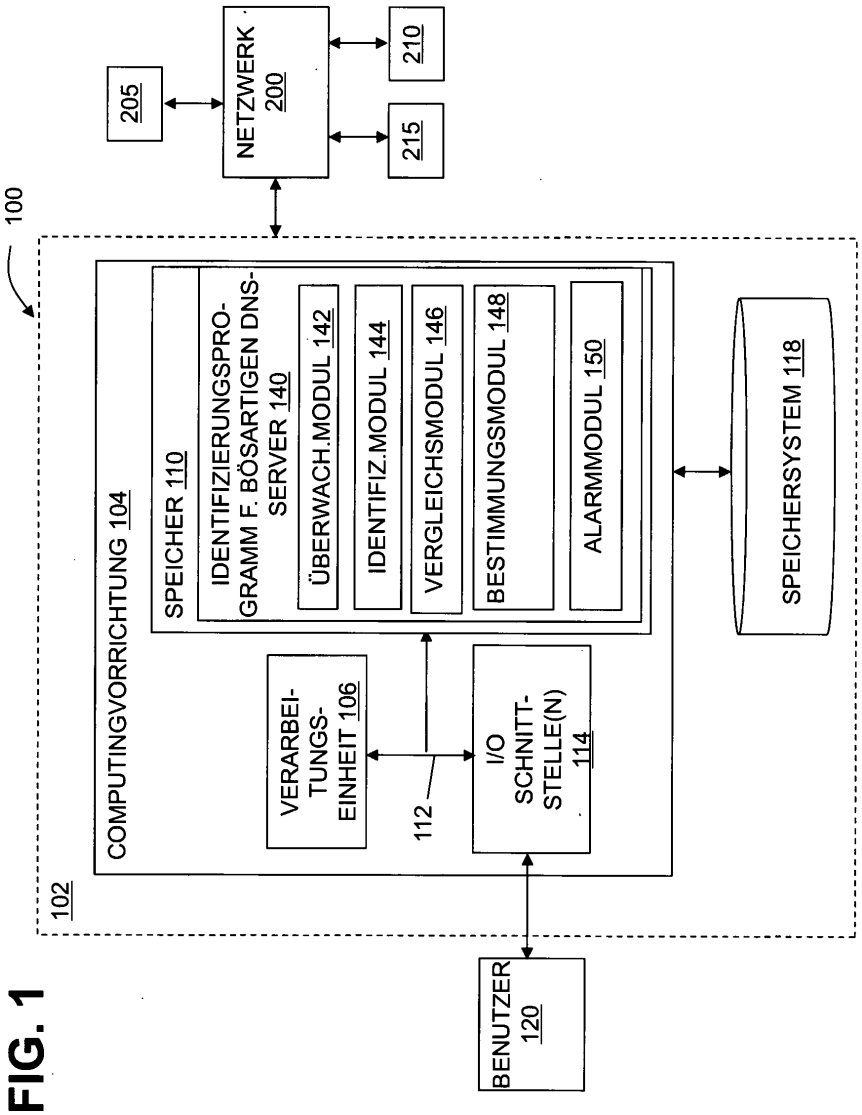


FIG. 1

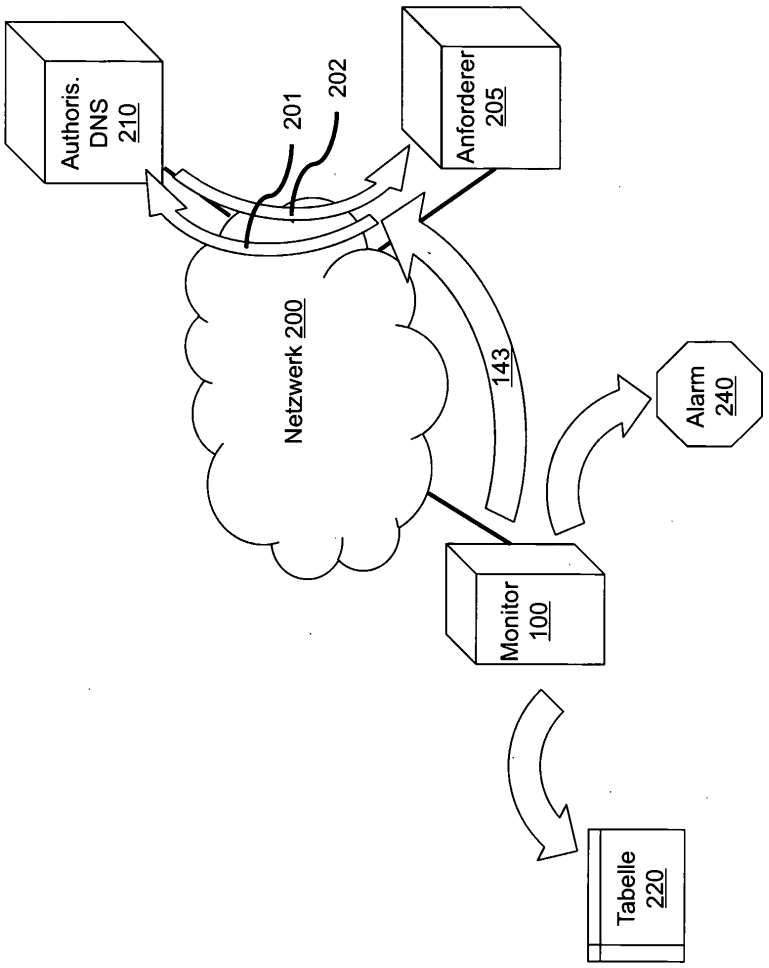

Authoris.
DNS
210
201
202
Anforderer
205
Netzwerk 200
143
Alarm
240
Monitor
100
Tabelle
220

FIG. 2

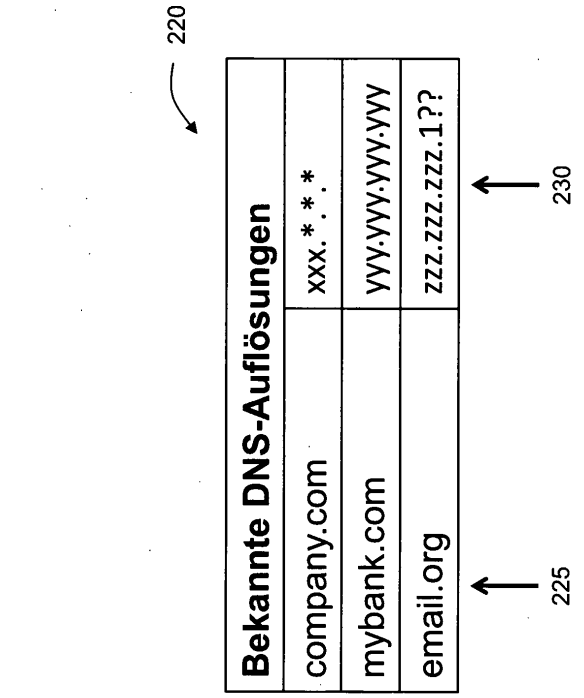

220
Bekannte DNS-Auflösungen
company.com
xxx.*.*.*
mybank.com
yyy.yyy.yyy.yyy
email.org
zzz.zzz.zzz.1??
225
230

FIG. 4

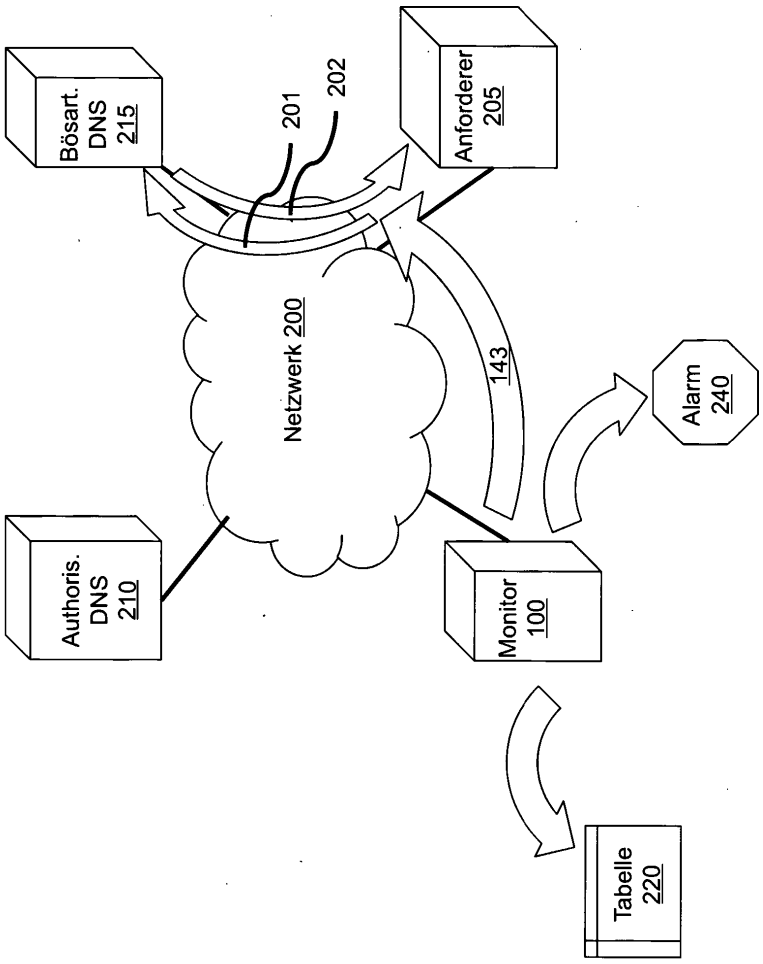
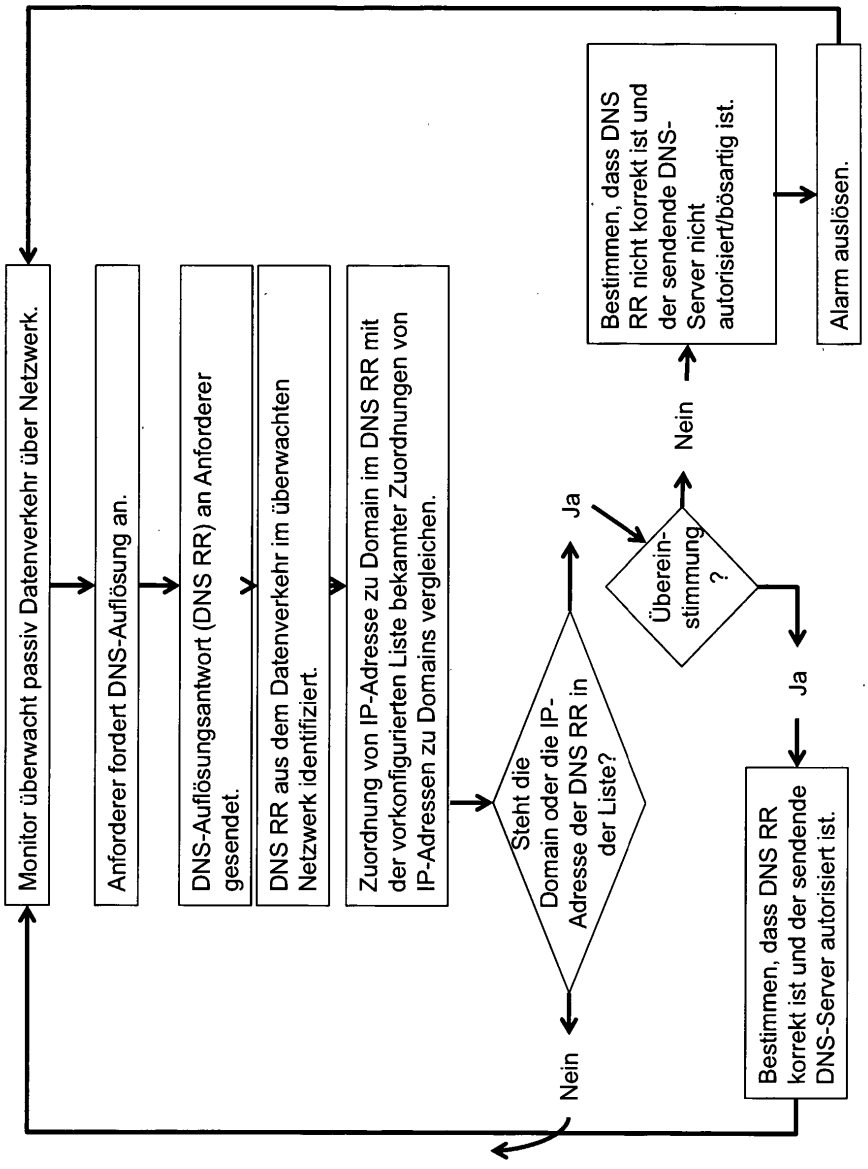

Bösart. DNS 215
201
202
Anforderer 205
Netzwerk 200
143
Alarm 240
Authoris. DNS 210
Monitor 100
Tabelle 220

FIG. 3

FIG. 5


Monitor überwacht passiv Datenverkehr über Netzwerk.
Anforderer fordert DNS-Auflösung an.
DNS-Auflösungsantwort (DNS RR) an Anforderer gesendet.
DNS RR aus dem Datenverkehr im überwachten Netzwerk identifiziert.
Zuordnung von IP-Adresse zu Domain im DNS RR mit der vorkonfigurierten Liste bekannter Zuordnungen von IP-Adressen zu Domains vergleichen.
Steht die Domain oder die IP-Adresse der DNS RR in der Liste?
Nein
Ja
Übereinstimmung?
Nein
Ja
Bestimmen, dass DNS RR nicht korrekt ist und der sendende DNS-Server nicht autorisiert/bösartig ist.
Alarm auslösen.
Bestimmen, dass DNS RR korrekt ist und der sendende DNS-Server autorisiert ist.

US009648033B2

(12) **United States Patent**
Crume

(10) **Patent No.: US 9,648,033 B2**
(45) **Date of Patent: *May 9, 2017**

(54) **SYSTEM FOR DETECTING THE PRESENCE OF ROGUE DOMAIN NAME SERVICE PROVIDERS THROUGH PASSIVE MONITORING**

(71) Applicant: **International Business Machines Corporation**, Armonk, NY (US)

(72) Inventor: **Jeffery L. Crume**, Raleigh, NC (US)

(73) Assignee: **International Business Machines Corporation**, Armonk, NY (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **14/884,899**

(22) Filed: **Oct. 16, 2015**

(65) **Prior Publication Data**

US 2016/0036845 A1 Feb. 4, 2016

Related U.S. Application Data

(63) Continuation of application No. 13/479,412, filed on May 24, 2012, now Pat. No. 9,225,731.

(51) **Int. Cl.**
H04L 29/06 (2006.01)
H04L 29/12 (2006.01)
H04L 12/26 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 63/1425*** (2013.01); ***H04L 61/10*** (2013.01); ***H04L 61/1511*** (2013.01);
(Continued)

(58) **Field of Classification Search**
None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

7,706,267 B2 * 4/2010 Ford et al. 370/230
7,756,933 B2 7/2010 Reshef et al.
(Continued)

FOREIGN PATENT DOCUMENTS

CN 101567815 A 10/2009
CN 102082836 A 6/2011
CN 102223422 A 10/2011

OTHER PUBLICATIONS

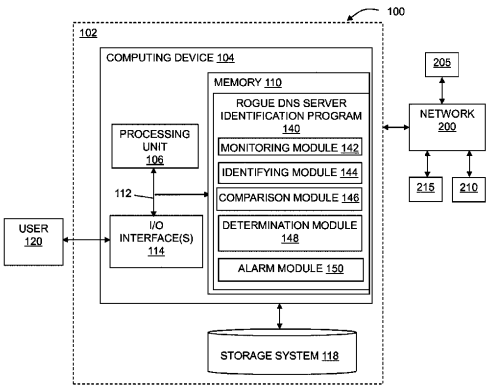
Chinese Patent Office, Office Action for CN 201310195777.3 dated Nov. 6, 2016, 9 pages.
(Continued)

Primary Examiner — Uzma Alam
(74) *Attorney, Agent, or Firm* — Daniel Simek; Hoffman Warnick LLC

(57) **ABSTRACT**

A method, system, computer program product embodied in a computer readable storage medium, and computer system are disclosed for identifying a rogue domain name service (DNS) server. Embodiments include passively monitoring traffic on a target network; and identifying a DNS resolution response in the traffic on the network. The DNS resolution response includes a mapping of a domain to an internet protocol (IP) address. The DNS resolution response is compared with a preconfigured list of known mappings of domains to IP addresses. Based on the results of the comparison, it can be determined whether the DNS resolution response is correct. In cases where the DNS resolution response is incorrect, the provider of the DNS resolution response is a rogue DNS server.

5 Claims, 5 Drawing Sheets



(52) **U.S. Cl.**
CPC ***H04L 63/1408*** (2013.01); ***H04L 63/1466*** (2013.01); ***H04L 63/1483*** (2013.01); *H04L 43/00* (2013.01)

(56) **References Cited**

U.S. PATENT DOCUMENTS

7,823,202	B1	10/2010	Nucci et al.	
7,873,993	B2	1/2011	King	
8,055,768	B2	11/2011	Saunderson et al.	
8,069,483	B1	11/2011	Matlock	
8,312,541	B2	11/2012	Levy-Abegnoli et al.	
8,370,933	B1 *	2/2013	Buckler	726/22
2004/0030796	A1	2/2004	Cooper et al.	
2004/0111640	A1	6/2004	Baum	
2006/0176822	A1 *	8/2006	Doyle et al.	370/241
2006/0253612	A1	11/2006	Cheshire	
2007/0186276	A1	8/2007	McRae et al.	
2007/0271220	A1 *	11/2007	Carter	707/2
2008/0060054	A1	3/2008	Srivastava	
2008/0147837	A1 *	6/2008	Klein et al.	709/223
2008/0307516	A1	12/2008	Levy-Abegnoli et al.	
2009/0327487	A1	12/2009	Olson et al.	
2010/0031362	A1	2/2010	Himberger et al.	
2010/0142709	A1	6/2010	Robert et al.	
2010/0262688	A1	10/2010	Hussain et al.	
2010/0291943	A1	11/2010	Mihaly et al.	
2011/0106919	A1	5/2011	Mazur et al.	
2011/0191455	A1 *	8/2011	Gardner	709/223
2011/0208838	A1 *	8/2011	Thomas et al.	709/219
2011/0214180	A1	9/2011	Gunawardena	
2011/0231931	A1	9/2011	Ma	
2011/0271345	A1	11/2011	Wolman et al.	
2012/0124087	A1 *	5/2012	Malan et al.	707/770
2013/0318170	A1	11/2013	Crume	
2013/0318605	A1	11/2013	Crume	
2013/0332986	A1 *	12/2013	Sima et al.	726/1
2013/0333038	A1 *	12/2013	Chien	726/23

OTHER PUBLICATIONS

Han et al.; "A Timing-Based Scheme for Rogue AP Detection", Parallel and Distributed Systems, IEEE Transactions on, vol. 22, Issue 11, Nov. 2011, pp. 1912-1925.

Dagon et al.; "Corrupted DNS Resolution Paths: The Rise of a Malicious Resolution Authority", ISC/OARC Workshop 2007, pp. 1-33.

Han et al.; "A Measurement Based Rogue AP Detection Scheme", INFOCOM IEEE, Apr. 19-25, 2009, pp. 1593-1601.

Caglayan et al.; "Real-Time Detection of Fast Flux Service Networks", CATCH'09 Cybersecurity Applications & Technology, IEEE, Mar. 3-4, 2009, pp. 285-292.

Mano et al.; "RIPPS: Rogue Identifying Packet Payload Slicer Detecting Unauthorized Wireless Hosts Through Network Traffic Conditioning", ACM Journal Name, vol. V. No. N. May 2007, pp. 1-2.

Hassan et al.; "Rogue DHCP Server Detection", retrieved from IP.com Prior Art Database, IP No. IPCOM000189334D, Nov. 5, 2009, 10 pages.

Qu et al.; "RaPiD: An Indirect Rogue Access Points Detection System", IPCCC IEEE 29th International Conference on, Dec. 9-11, 2010, pp. 9-16.

Beyah et al.; "Rogue-Access-Point Detection: Challenges, Solutions, and Future Directions", Security & Privacy, IEEE, Sep.-Oct. 2011, vol. 9, Iss. 5, pp. 56-61.

Alam, Office Action Communication for U.S. Appl. No. 13/479,412 dated Jul. 2, 2014, 34 pages.

Alam, Office Action Communication for U.S. Appl. No. 13/479,412 dated Jan. 27, 2015, 19 pages.

Alam, Notice of Allowance and Fee(s) Due for U.S. Appl. No. 13/479,412 dated Jul. 17, 2015, 6 pages.

Application No. DE 10 2013 208 923.6, Office Action dated Jan. 27, 2014, 12 pages.

Torres-Diaz, Office Action Communication for U.S. Appl. No. 13/479,418, dated Jul. 2, 2014, 13 pages.

Torres-Diaz, Office Action Communication for U.S. Appl. No. 13/479,418 dated Nov. 5, 2014, 14 pages.

Torres-Diaz, Office Action Communication for U.S. Appl. No. 13/479,418 dated Nov. 26, 2013, 11 pages.

Torres-Diaz, Office Action Communication for U.S. Appl. No. 13/479,418 dated May 9, 2013, 17 pages.

* cited by examiner

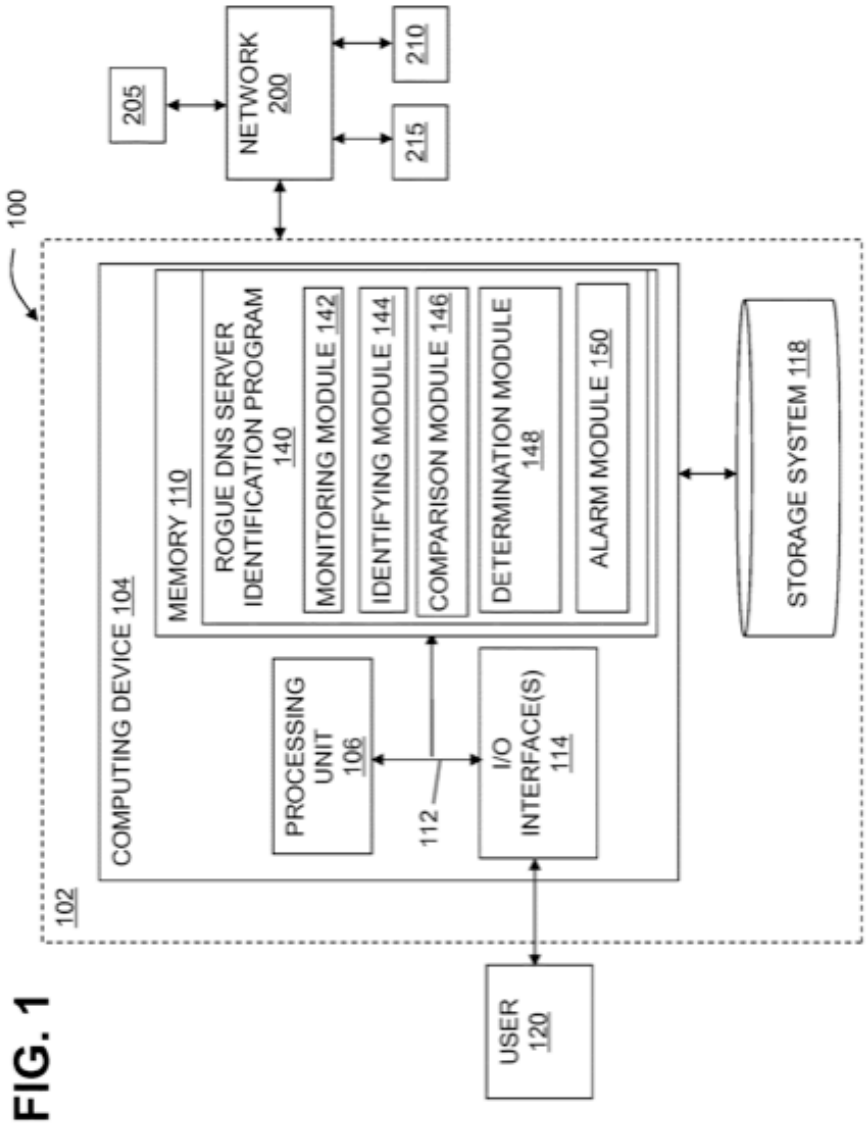

100
102
205
NETWORK 200
210
215
COMPUTING DEVICE 104
MEMORY 110
ROGUE DNS SERVER IDENTIFICATION PROGRAM 140
MONITORING MODULE 142
IDENTIFYING MODULE 144
COMPARISON MODULE 146
DETERMINATION MODULE 148
ALARM MODULE 150
PROCESSING UNIT 106
112
I/O INTERFACE(S) 114
STORAGE SYSTEM 118
USER 120

FIG. 1

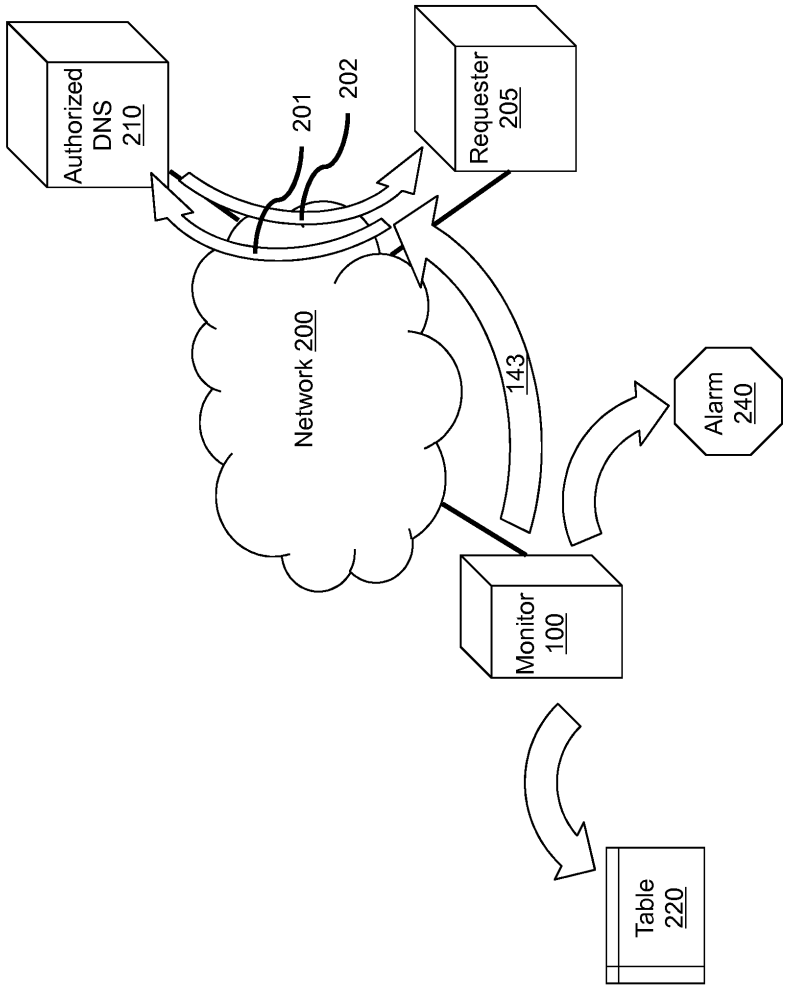

Authorized DNS 210
201
202
Requester 205
Network 200
143
Alarm 240
Monitor 100
Table 220

FIG. 2

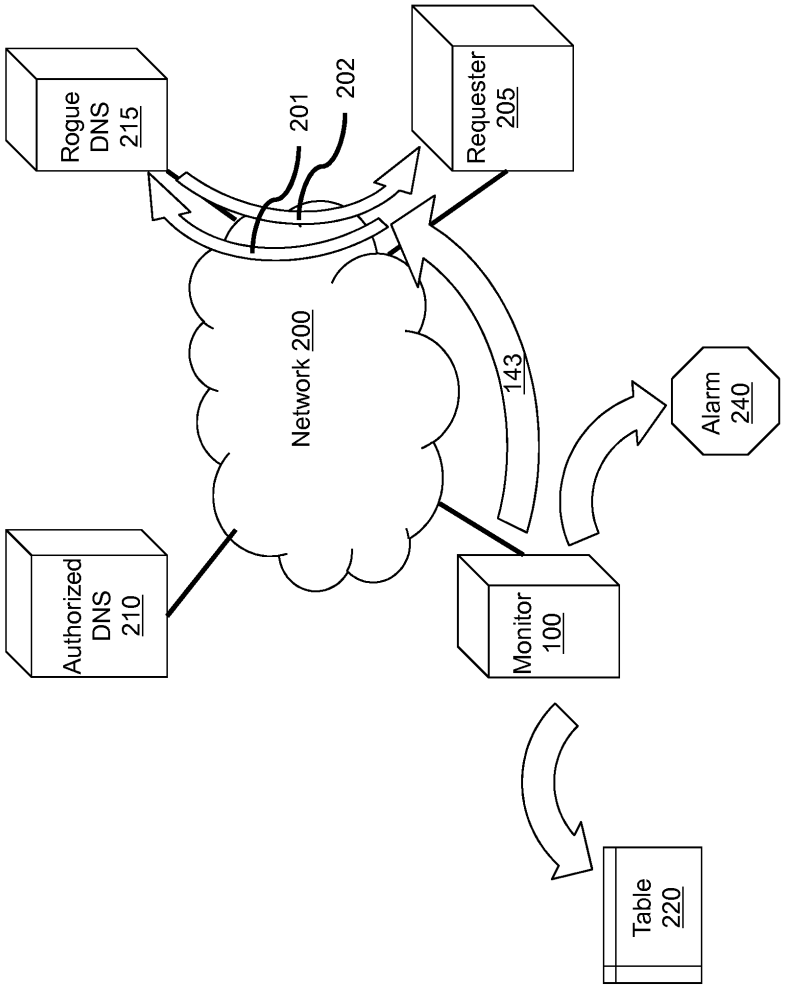

Rogue DNS 215
201
202
Requester 205
Network 200
143
Alarm 240
Authorized DNS 210
Monitor 100
Table 220

FIG. 3

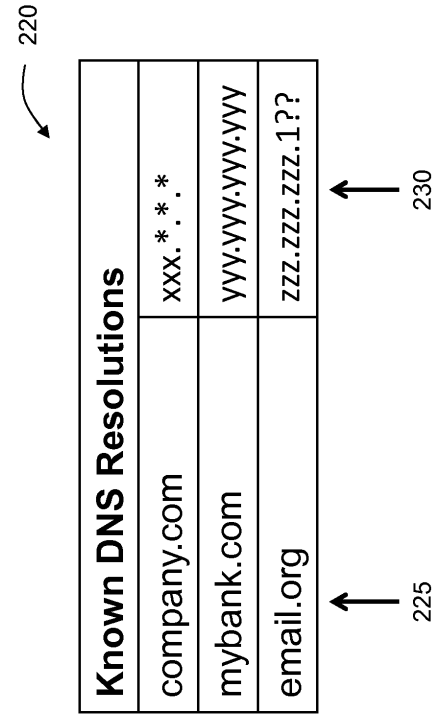

220
Known DNS Resolutions
company.com
xxx.*.*.*
mybank.com
yyy.yyy.yyy.yyy
email.org
zzz.zzz.zzz.1??
225
230

FIG. 4

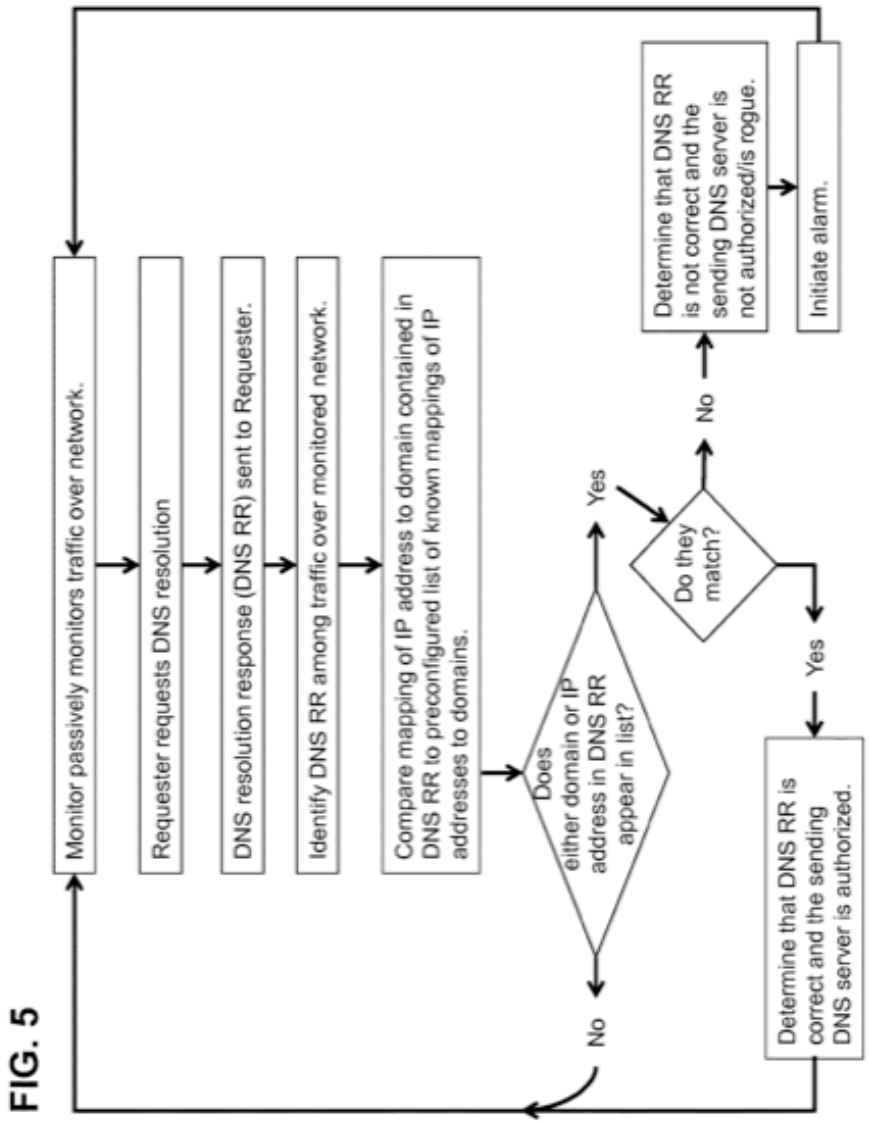

Monitor passively monitors traffic over network.
Requester requests DNS resolution
DNS resolution response (DNS RR) sent to Requester.
Identify DNS RR among traffic over monitored network.
Compare mapping of IP address to domain contained in DNS RR to preconfigured list of known mappings of IP addresses to domains.
Does either domain or IP address in DNS RR appear in list?
Yes
No
Do they match?
Yes
No
Determine that DNS RR is correct and the sending DNS server is authorized.
Determine that DNS RR is not correct and the sending DNS server is not authorized/is rogue.
Initiate alarm.

FIG. 5

SYSTEM FOR DETECTING THE PRESENCE OF ROGUE DOMAIN NAME SERVICE PROVIDERS THROUGH PASSIVE MONITORING

TECHNICAL FIELD

The invention relates generally to identifying untrusted or compromised sources for network information. More particularly, the invention relates to identifying rogue DNS servers via passive monitoring.

BACKGROUND

The Domain Name Service (DNS) resolves alphanumeric domain names into numeric IP addresses. This service is provided by a loose collection of servers scattered around the Internet as well as within local Intranets. If, however, the information supplied through this service comes not from an authorized source, but rather, an attacker's system supplying incorrect information or from an authorized source that has been compromised, network traffic could be impeded in a denial of service (DOS) attack or misrouted in a spoofing or man-in-the-middle attack. This could result in sensitive traffic being delivered to untrusted systems or not being delivered at all.

One way that these services could be subverted would be if an attacker set up an "evil twin" WiFi hotspot which impersonates a trusted wireless access point and establishes itself as a man-in-the-middle (MITM), which reroutes network traffic. The MITM can examine and modify all traffic coming into and going out of the rogue network. Another way would be for the attacker to set up a rogue server which hijacks network services by broadcasting to all nodes in the network that it is online and available to process DNS requests. Yet another way would be for an attacker to compromise a trusted DNS server and cause it to produce erroneous results. In many cases, the last server to broadcast will be considered authoritative by other nodes in the network.

One solution for detecting such untrusted or compromised sources of network information is the use of a DNS watcher which performs a "health check" by polling a preconfigured list of trusted DNS servers to verify that they are operational and are returning proper results. There are several drawbacks to this method, however. Polling operations generate additional, superfluous network traffic, and may be discovered by an attacker's reconnaissance of the target network. A polling approach also only verifies whether known DNS servers are performing properly. By virtue of the active nature of polling specific known DNS servers, it is unable to verify the correctness of DNS resolutions returned by hosts other than the known hosts being polled. Since rogue DNS providers would not be known in advance, they would go unchecked by a polling solution.

BRIEF DESCRIPTION

In general, aspects of the present invention provide a passive monitoring solution for identifying a rogue DNS server in a network which does not generate additional network traffic, and is able to monitor DNS resolutions provided by both known and unknown DNS servers.

A first aspect of the disclosure provides a method for identifying a rogue domain name service (DNS) server. The method comprises: passively monitoring traffic on a network; identifying a DNS resolution response in the traffic on the network, wherein the DNS resolution response includes a mapping of a domain to an internet protocol (IP) address; comparing the DNS resolution response with a preconfigured list of known mappings of domains to IP addresses; and determining whether the DNS resolution response is correct based on the comparing.

A second aspect of the disclosure provides a system for identifying a rogue domain name service (DNS) server. The system comprises: a monitoring component for passively monitoring traffic on a network; an identification component for identifying a DNS resolution response in the traffic on the network, wherein the DNS resolution response includes a mapping of a domain to an internet protocol (IP) address; a comparison component for comparing the DNS resolution response with a preconfigured list of known mappings of domains to IP addresses; and a determination component for determining whether the DNS resolution response is correct based on the comparing.

A third aspect of the disclosure provides a computer program product embodied in a computer readable storage medium which, when executed by a computing device, causes the computer system to implement a method for identifying a rogue domain name service (DNS) server. The method comprises: passively monitoring traffic on a network; identifying a DNS resolution response in the traffic on the network, wherein the DNS resolution response includes a mapping of a domain to an internet protocol (IP) address; comparing the DNS resolution response with a preconfigured list of known mappings of domains to IP addresses; and determining whether the DNS resolution response is correct based on the comparing.

These and other aspects, advantages and salient features of the invention will become apparent from the following detailed description, which, when taken in conjunction with the annexed drawings, where like parts are designated by like reference characters throughout the drawings, disclose embodiments of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** shows a data processing system suitable for implementing an embodiment of the invention.

FIG. **2** shows a schematic data flow diagram illustrating monitoring of a network according to an embodiment of the invention.

FIG. **3** shows a schematic data flow diagram illustrating identification of a rogue

DNS server according to an embodiment of the invention.

FIG. **4** shows a preconfigured DNS resolution table in accordance with an embodiment of the invention.

FIG. **5** shows a flow chart for a method of identifying a rogue DNS server in accordance with an embodiment of the invention.

The drawings are not necessarily to scale. The drawings are merely schematic representations, not intended to portray specific parameters of the invention. The drawings are intended to depict only typical embodiments of the invention, and therefore should not be considered as limiting the scope of the invention. In the drawings, like numbering represents like elements.

DETAILED DESCRIPTION OF THE INVENTION

As indicated above, aspects of the present invention provide a solution for detecting the presence of rogue DNS servers through the use of a monitor which passively

observes the flow of traffic across a network between nodes, and looks for spoofed DNS traffic in that network. In some embodiments, the network may be a local Intranet, and in others, the network may be the Internet.

Turning to the drawings, FIG. **1** shows an illustrative monitor **100** for detecting the presence of rogue DNS servers **215** that may be present in network **200**. To this extent, monitor **100** includes a computer system **102** that can perform a process described herein in order to identify an invalid DNS resolution response from a rogue DNS server **215**. In particular, computer system **102** is shown including a computing device **104** that includes a rogue DNS server identification program **140**, which makes computing device **104** operable to identify a rogue DNS server **215** by performing a process described herein.

Computing device **104** is shown including a processing unit **106** (e.g., one or more processors), a memory **110**, a storage system **118** (e.g., a storage hierarchy), an input/output (I/O) interface component **114** (e.g., one or more I/O interfaces and/or devices), and a communications pathway **112**. In general, processing unit **106** executes program code, such as rogue DNS server identification program **140**, which is at least partially fixed in memory **110**. To this extent, processing unit **106** may comprise a single processing unit, or be distributed across one or more processing units in one or more locations.

Memory **110** can also include local memory, employed during actual execution of the program code, bulk storage (storage **118**), and/or cache memories (not shown) which provide temporary storage of at least some program code in order to reduce the number of times code must be retrieved from bulk storage **118** during execution. As such, memory **110** may comprise any known type of data storage and/or transmission media, including magnetic media, optical media, random access memory (RAM), read-only memory (ROM), a data cache, a data object, etc. Moreover, similar to processing unit **116**, memory **110** may reside at a single physical location, comprising one or more types of data storage, or be distributed across a plurality of physical systems in various forms.

While executing program code, processing component **106** can process data, which can result in reading and/or writing transformed data from/to memory **110** and/or I/O component **114** for further processing. Pathway **112** provides a direct or indirect communications link between each of the components in computer system **102**. I/O interface component **114** can comprise one or more human I/O devices, which enable a human user **120** to interact with computer system **102** and/or one or more communications devices to enable a system user **120** to communicate with computer system **102** using any type of communications link.

To this extent, rogue DNS server identification program **140** can manage a set of interfaces (e.g., graphical user interface(s), application program interface, and/or the like) that enable human and/or system users **120** to interact with rogue DNS server identification program **140**. Further, rogue DNS server identification program **140** can manage (e.g., store, retrieve, create, manipulate, organize, present, etc.) the data, such as data stored in table **220** (FIGS. **2-4**), using any solution.

In any event, computer system **102** can comprise one or more general purpose computing articles of manufacture **104** (e.g., computing devices) capable of executing program code, such as rogue DNS server identification program **140**, installed thereon. As used herein, it is understood that "program code" means any collection of instructions, in any language, code or notation, that cause a computing device having an information processing capability to perform a particular action either directly or after any combination of the following: (a) conversion to another language, code or notation; (b) reproduction in a different material form; and/or (c) decompression. To this extent, rogue DNS server identification program **140** can be embodied as any combination of system software and/or application software. In any event, the technical effect of computer system **102** is to provide processing instructions to computing device **104** in order to identify a rogue DNS server.

Further, rogue DNS server identification program **140** can be implemented using a set of modules **142-150**. In this case, a module **142-150** can enable computer system **102** to perform a set of tasks used by rogue DNS server identification program **140**, and can be separately developed and/or implemented apart from other portions of rogue DNS server identification program **140**. As used herein, the term "component" means any configuration of hardware, with or without software, which implements the functionality described in conjunction therewith using any solution, while the term "module" means program code that enables a computer system **102** to implement the actions described in conjunction therewith using any solution. When fixed in a memory **110** of a computer system **102** that includes a processing component **106**, a module is a substantial portion of a component that implements the actions. Regardless, it is understood that two or more components, modules, and/or systems may share some/all of their respective hardware and/or software. Further, it is understood that some of the functionality discussed herein may not be implemented or additional functionality may be included as part of computer system **102**.

When computer system **102** comprises multiple computing devices **104**, each computing device **104** can have only a portion of rogue DNS server identification program **140** fixed thereon (e.g., one or more modules **142-150**). However, it is understood that computer system **102** and rogue DNS server identification program **140** are only representative of various possible equivalent computer systems that may perform a process described herein. To this extent, in other embodiments, the functionality provided by computer system **102** and rogue DNS server identification program **140** can be at least partially implemented by one or more computing devices that include any combination of general and/or specific purpose hardware with or without program code. In each embodiment, the hardware and program code, if included, can be created using standard engineering and programming techniques, respectively.

When computer system **102** includes multiple computing devices **104**, the computing devices can communicate over any type of communications link. Further, while performing a process described herein, computer system **102** can communicate with one or more other computer systems using any type of communications link. In either case, the communications link can comprise any combination of various types of wired and/or wireless links; comprise any combination of one or more types of networks; and/or utilize any combination of various types of transmission techniques and protocols.

As discussed herein, rogue DNS server identification program **140** enables computer system **102** to implement identification of a rogue DNS server. To this extent, rogue DNS server identification program **140** is shown including a monitoring module **142**, an identifying module **144**, a comparison module **146**, a determination module **148**, and an alarm module **150**.

Referring now to FIGS. **2-3**, the network environment **200** in which monitor **100** may be used is depicted. As illustrated, network **200** may include a requester **205**, which may be a client workstation operated by a user or a server. Additional requesters **205** may be included in network **200**, but are omitted from the depiction of network **200** in FIGS. **2-3** for simplicity. Requester **205** may send a DNS resolution request **201** for resolution of a particular host's alphanumeric domain name into a numeric IP address.

As shown in FIG. **2**, under normal operating conditions, in which an attacker is not present in network **200**, DNS resolution request **201** is received and processed by authorized DNS server **210**, which sends DNS resolution response **202**. In that case, DNS resolution response **202** may contain a valid and accurate mapping of domain name to IP address.

In other cases, as shown in FIG. **3**, an attacker's rogue DNS sever **215** may be present in network **200** with the purpose of impersonating another computing system. In this case, DNS resolution request **201** is received and processed by rogue DNS server **215**, and DNS resolution response **202** is provided by rogue DNS server **215**. Such a DNS resolution response **202** may contain an incorrect domain name to IP address mapping, resulting in either misrouting of network traffic in a spoofing attack in which sensitive traffic is delivered to an untrusted system, or impeding of network traffic in a denial of service (DOS) attack.

In either case, monitor **100** is positioned at a strategic point in network **200** such that monitor **100** can observe the flow of network traffic between nodes on network **200**. As discussed above with reference to FIG. **1**, monitor **100** includes modules **142-150**, which when executed by computer system **102**, perform passive monitoring of traffic on network **200**, including, among other network traffic, DNS resolution requests **201** and DNS resolution responses **202**.

Referring concurrently to FIGS. **1-3**, monitoring module **142**, part of monitor **100**, performs monitoring **143** of traffic across network **200**, including DNS resolution requests **201** and DNS resolution responses **202**. Identification component **144** can identify, in the traffic monitored on the network **200**, a DNS resolution response **202**. As mentioned previously, a DNS resolution response **202** includes a mapping of a domain name **225** to an IP address **230** in response to a DNS resolution request **201** sent by requester **205**.

Once a DNS resolution response **202** is identified, comparison module **146** can perform a comparison of the DNS resolution response **202** with the known mappings stored in a preconfigured list of known mappings of domain names and IP addresses contained in a known DNS resolution table **220**. The mappings of domain names to IP addresses contained in table **220** are known to be valid. As shown in FIG. **4**, the IP address **230** stored in table **220** may be expressed as a specific IP address, such as yyy.yyy.yyy.yyy, the IP address of the domain mybank.com. In other embodiments, IP addresses **230** stored in table **200** may be expressed as a range of IP addresses using at least one wild card. A range of IP addresses may be broad, including several wild cards such as, for example, xxx.*.*.*, the IP address range for the domain company.com. In other embodiments the range of IP addresses may be narrower, for example having only one wild card, such as zzz.zzz.zzz.1??, the IP address range for the domain email.org.

According to embodiments of the invention, the list of mapped domain names **225** and IP addresses **230** stored in table **220** need not be an exhaustive list of domains that a user of network **200** may access, or for which requester **205** may request DNS resolutions. Rather, a selected number of hosts may be included in table **220** as a representative sample. In some embodiments, table **220** may include a preconfigured list of domains and their respective IP addresses whose selection for inclusion in table **220** is based on the domain hosting particularly sensitive information accessed by network users. In other embodiments, table **220** may include a preconfigured list of domains and their respective IP addresses whose selection for inclusion in table **220** is based on a high frequency of visits by users of network **200**, and therefore a high likelihood of a large sample pool of DNS resolution requests and responses to monitor.

Referring back to FIGS. **1-3**, determination module **148** performs a determination of whether the DNS resolution response **202** contains a correct and valid mapping of IP address to domain name. This determination is based on the comparison performed by comparison module **146**. Where the mapping in DNS resolution response **202** matches the mapping for the respective domain name stored in table **220**, DNS resolution response **202** is determined to be correct. This would indicate that DNS resolution response **202** may have been sent by authorized DNS server **210** (FIG. **2**). Where the mapping in DNS resolution response **202** does not match the mapping for the respective domain name in table **220**, DNS resolution response **202** is determined to be invalid. This would indicate that DNS resolution response **202** may have been sent by rogue DNS server **215** (FIG. **3**), and may indicate the occurrence of either a spoof or DOS attack. In this case, alarm module **150** sends an alarm **240** to advise requester **205** of the spoofed DNS traffic. In various embodiments, alarm **240** may take the form of a message (email, SMS, etc.), a log entry, or other form of security event notification which documents and draws attention to the suspicious behavior.

The foregoing method is depicted in a flow chart in FIG. **5**. As previously described, a monitor passively monitors traffic over a network. Over this network, a requesting workstation requests a DNS resolution of a particular domain. A DNS resolution response is returned to the Requester over the network by a DNS server. The DNS resolution response is identified by the monitor among the monitored network traffic. Once identified, the mapping of an IP address to a domain contained in the DNS resolution response is compared to a preconfigured list of known mappings of IP addresses to domains. If neither the domain nor the IP address in the DNS resolution response appears in the preconfigured list of known mappings of IP addresses to domains, the monitor simply returns to monitoring the network.

If either the domain or the IP address in the DNS resolution response appears in the preconfigured list of known mappings of IP addresses to domains, the mapping contained in the DNS resolution request is compared to the corresponding mapping in the preconfigured list of known mappings of IP addresses to domains. If the mapping matches, i.e. both the IP address and the respective domain are the same in the DNS resolution response and the preconfigured list of known mappings of IP addresses to domains, then it can be determined that the DNS resolution response is correct and the DNS server that sent it is authorized. If, however, the mapping does not match, i.e., the domain corresponds to different IP addresses in the DNS resolution response and the preconfigured list of known mappings of IP addresses to domains (or the IP address corresponds to different domains in the DNS resolution response and the preconfigured list of known mappings of IP addresses to domains), then it can be determined that the DNS resolution response is invalid. In such a case, it can be

concluded that the DNS server that sent it is not authorized, and may be a rogue DNS server. In this instance, an alarm is initiated, alerting the requester to the security risk.

While shown and described herein as a method and system for identifying a rogue DNS server, it is understood that aspects of the invention further provide various alternative embodiments. For example, in one embodiment, the invention provides a computer program fixed in at least one computer-readable medium, which when executed, enables a computer system to implement identification of a rogue DNS server, To this extent, the computer-readable medium includes program code, such as rogue DNS server identification program **140** (FIG. **1**), which implements some or all of a process described herein. It is understood that the term "computer-readable medium" comprises one or more of any type of tangible medium of expression, now known or later developed, from which a copy of the program code can be perceived, reproduced, or otherwise communicated by a computing device. For example, the computer-readable medium can comprise: one or more portable storage articles of manufacture; one or more memory/storage components of a computing device; paper; and/or the like.

In another embodiment, the invention provides a method of providing a copy of program code, such as rogue DNS server identification program **140** (FIG. **1**), which implements some or all of a process described herein. In this case, a computer system can process a copy of program code that implements some or all of a process described herein to generate and transmit, for reception at a second, distinct location, a set of data signals that has one or more of its characteristics set and/or changed in such a manner as to encode a copy of the program code in the set of data signals. Similarly, an embodiment of the invention provides a method of acquiring a copy of program code that implements some or all of a process described herein, which includes a computer system receiving the set of data signals described herein, and translating the set of data signals into a copy of the computer program fixed in at least one computer-readable medium. In either case, the set of data signals can be transmitted/received using any type of communications link.

In still another embodiment, the invention provides a method of generating a system for identifying a rogue DNS server. In this case, a computer system, such as computer system **102** (FIG. **1**), can be obtained (e.g., created, maintained, made available, etc.) and one or more components for performing a process described herein can be obtained (e.g., created, purchased, used, modified, etc.) and deployed to the computer system. To this extent, the deployment can comprise one or more of: (1) installing program code on a computing device; (2) adding one or more computing and/or I/O devices to the computer system; (3) incorporating and/or modifying the computer system to enable it to perform a process described herein; and/or the like.

As used herein, the terms "first," "second," and the like, do not denote any order, quantity, or importance, but rather are used to distinguish one element from another, and the terms "a" and "an" herein do not denote a limitation of quantity, but rather denote the presence of at least one of the referenced item. The modifier "about" used in connection with a quantity is inclusive of the stated value and has the meaning dictated by the context (e.g., includes the degree of error associated with measurement of the particular quantity). The suffix "(s)" as used herein is intended to include both the singular and the plural of the term that it modifies, thereby including one or more of that term (e.g., the server(s) includes one or more server). Ranges disclosed herein are inclusive and independently combinable (e.g., ranges of "up to about 3 wild cards, or, more specifically, about 1 wild cards to about 3 wild cards," is inclusive of the endpoints and all intermediate values of the ranges of "about 1 wild card to about 2 wild cards," etc.).

The descriptions of the various embodiments of the present invention have been presented for purposes of illustration, but are not intended to be exhaustive or limited to the embodiments disclosed. Many modifications and variations will be apparent to those of ordinary skill in the art without departing from the scope and spirit of the described embodiments. The terminology used herein was chosen to best explain the principles of the embodiments, the practical application or technical improvement over technologies found in the marketplace, or to enable others of ordinary skill in the art to understand the embodiments disclosed herein.

What is claimed is:

1. A computer system comprising a non-transitory computer readable storage device, one or more processors, and program code stored on the non-transitory computer readable storage device for execution by the one or more processors to perform a method comprising:

passively monitoring traffic on a network;

identifying a DNS resolution response in the traffic on the network, wherein the DNS resolution response includes a mapping of a domain to an internet protocol (IP) address;

comparing the DNS resolution response with a preconfigured list of known mappings of domains to IP addresses,

wherein each IP address in the preconfigured list of known mappings of domains to IP addresses is a range of IP addresses expressed using at least one wild card;

determining whether the DNS resolution response is correct based on the comparing; and

sending an alarm in a case in which the DNS resolution response is determined to be incorrect.

2. The computer system of claim **1**, wherein the alarm comprises at least one of an email message, an SMS message, a log entry, or a security event notification.

3. The computer system of claim **1**, wherein the preconfigured list of known mappings of domains and IP addresses further includes a preconfigured list of domains most frequently visited by users of a network.

4. The computer system of claim **1**, wherein the preconfigured list of known mappings of domains and IP addresses further includes a preconfigured list of domains hosting sensitive information accessed by network users.

5. The computer system of claim **1**, wherein the network includes an intranet.

* * * * *

9.9 Migration Across Authentication Systems

US 20100269151A1

(19) **United States**

(12) **Patent Application Publication**

(10) **Pub. No.: US 2010/0269151 A1**

(43) **Pub. Date: Oct. 21, 2010**

Crume

(54) **MIGRATION ACROSS AUTHENTICATION SYSTEMS**

(76) Inventor: **Jeffery L. Crume**, Raleigh, NC (US)

Correspondence Address:
HOFFMAN WARNICK LLC
75 STATE ST, 14 FL
ALBANY, NY 12207 (US)

(21) Appl. No.: **12/426,365**

(22) Filed: **Apr. 20, 2009**

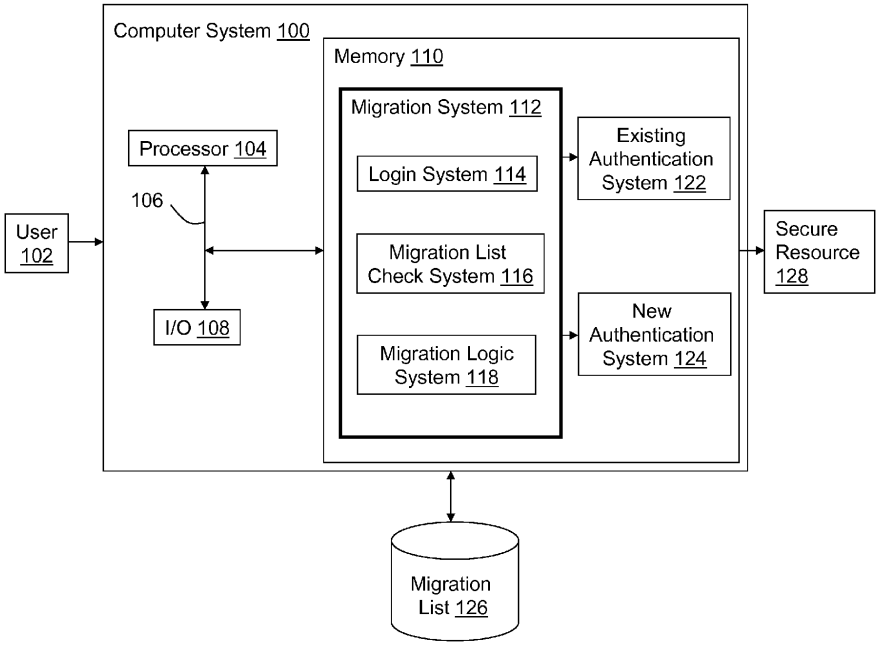
Publication Classification

(51) **Int. Cl.**
H04L 9/00 (2006.01)

(52) **U.S. Cl.** **726/2**

(57) **ABSTRACT**

A system, method, program product and a method for deploying a system for providing migration across authentication systems are disclosed. A system is provided that includes a login system that collects information from a user during a login process, a migration list check system that compares the information to a migration list to determine if the user is selected for migration, and a migration logic system that migrates the user from the existing authentication system to the new authentication system during the login process if the user is selected.



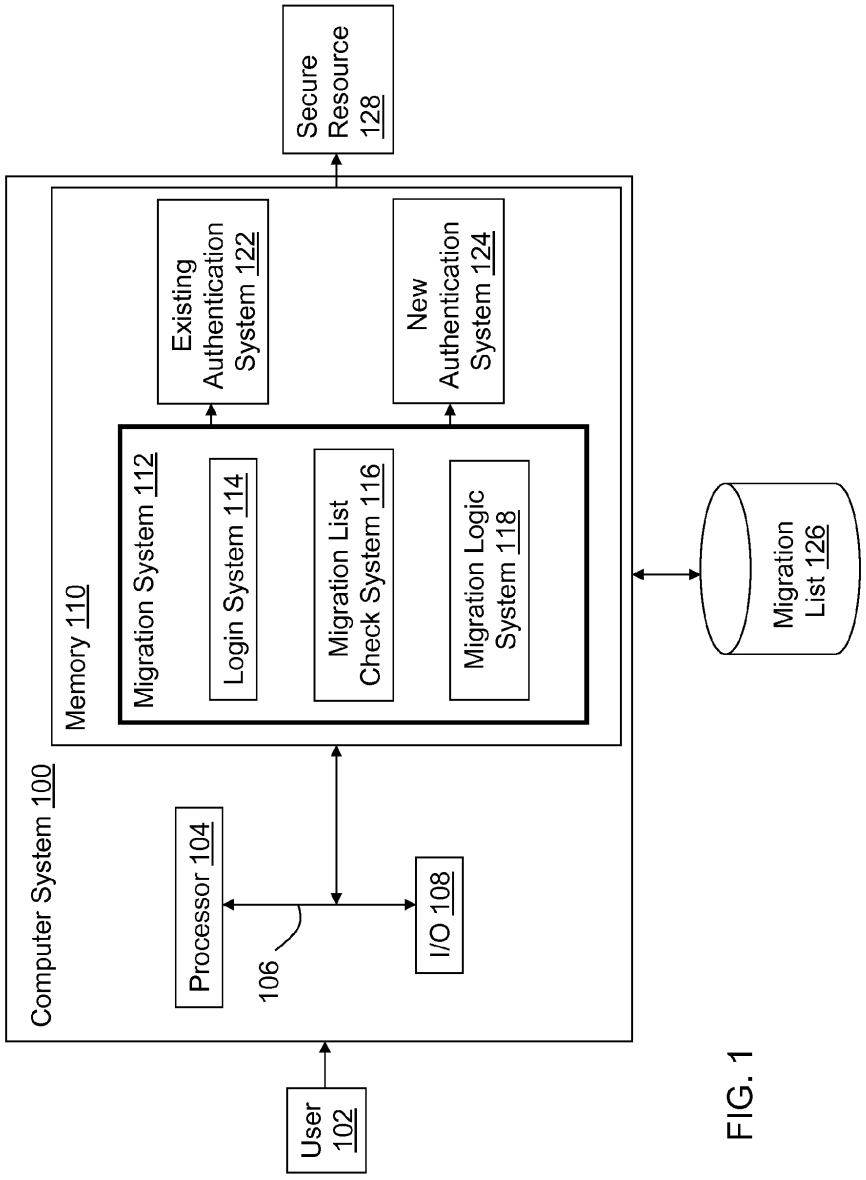

Secure Resource 128
Existing Authentication System 122
New Authentication System 124
Memory 110
Migration System 112
Login System 114
Migration List Check System 116
Migration Logic System 118
Migration List 126
Computer System 100
Processor 104
106
I/O 108
User 102

FIG. 1

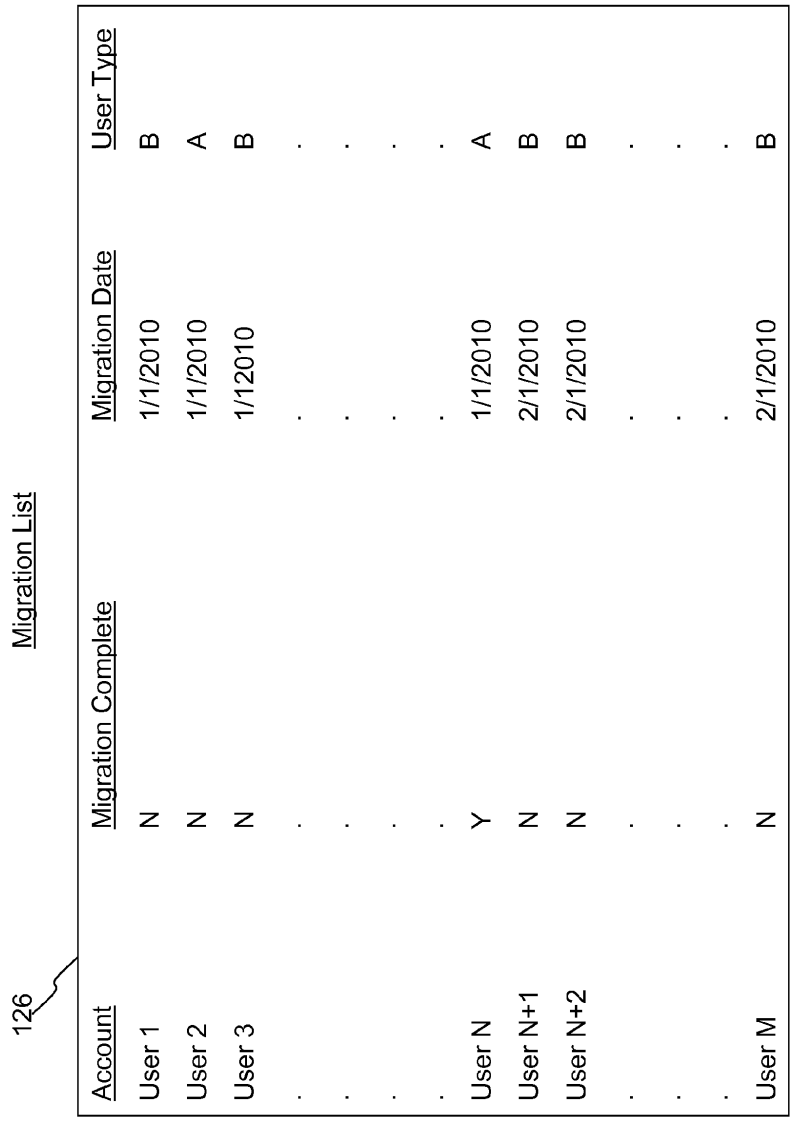

126
Migration List
Account
Migration Complete
Migration Date
User Type
User 1
N
1/1/2010
B
User 2
N
1/1/2010
A
User 3
N
1/12010
B
User N
Y
1/1/2010
A
User N+1
N
2/1/2010
B
User N+2
N
2/1/2010
B
User M
N
2/1/2010
B

FIG. 2

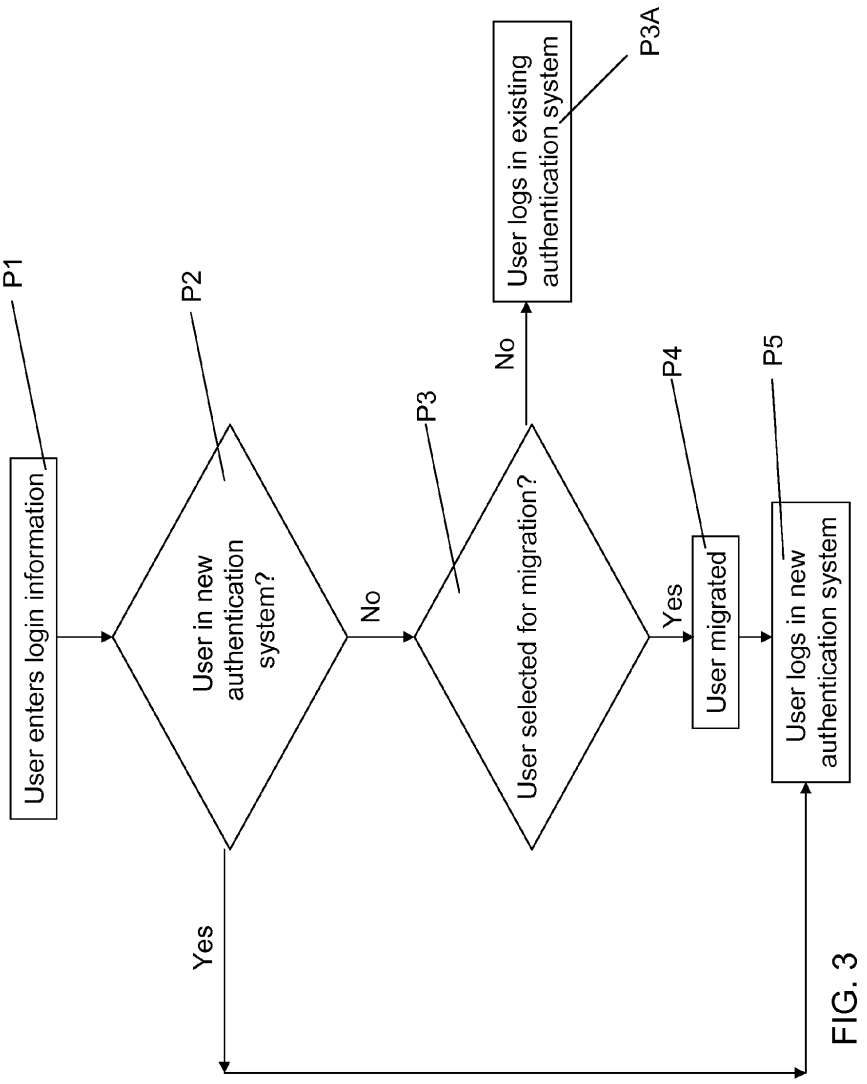

P1
User enters login information
P2
User in new authentication system?
Yes
No
P3
User selected for migration?
No
P3A
User logs in existing authentication system
Yes
P4
User migrated
P5
User logs in new authentication system

FIG. 3

MIGRATION ACROSS AUTHENTICATION SYSTEMS

FIELD OF THE INVENTION

[0001] This disclosure relates to the migration of users across authentication systems, and more specifically discloses a system, method, program product and a method for deploying a system for the selective, secure and transparent migration of users across authentication systems.

BACKGROUND OF THE INVENTION

[0002] Authentication systems are widely used by websites to authenticate a user. For example, an authentication system may be used to provide access to a secure resource. A secure resource may, for example, include: customer data, financial information or retirement accounts. Occasionally, websites may also implement new authentication systems to, for example, upgrade security, replace legacy systems and provide additional services to their customers. The migration of users from one authentication system to another introduces certain challenges. As an example, users are typically required to change their password or re-register because credentials are not typically transferable. In addition, there may be a desire to have a phased migration when a new authentication system is introduced. A phased migration allows for the conservation of resources, the ability to monitor the migration in a controlled environment, the ability to stop, increase or decrease the migration and the ability to select the number, or group, of users to be migrated.

[0003] In a typical migration, a user logs into an existing authentication system and is directed to a new authentication system. The user then typically has to login again or provide supplemental information before reaching the new authentication system. The additional information required from the user, as an example, may be in the form of re-entering a user identification and password, creating a new password, or providing some other information to confirm the authenticity of the user.

[0004] The additional time and effort required by the user for entering this information or the need to provide and then remember a new user identification and password is often an inconvenience and a barrier to a user attempting to reach a new authentication system.

SUMMARY OF THE INVENTION

[0005] A system, method, program product and a method for deploying a system for providing migration across authentication systems are disclosed. In one embodiment, there is a migration system that includes a login system that collects information from a user, a migration list check system that compares the user to a migration list to determine if the user is selected for migration and a migration logic system that migrates the user from the existing authentication system to the new authentication system during the login process if the user is selected.

[0006] In a second embodiment, there is a computer readable medium having a program product stored therein for migrating a user from an existing authentication system to a new authentication system, comprising program code for collecting information from the user during a login process, program code for comparing the information to a migration list to determine if the user is selected for migration, and program code for migrating the user from the existing authentication system to the new authentication system during the login process if the user is selected.

[0007] In a third embodiment, there is a method of migrating a user from an existing authentication system to a new authentication system, comprising collecting information from the user during a login process, comparing the information to a migration list to determine if the user is selected for migration, and migrating the user from the existing authentication system to the new authentication system during the login process if the user is selected.

[0008] In a fourth embodiment, there is a method for deploying a system for migrating a user from an existing authentication system to a new authentication system, comprising providing a computer infrastructure being operable to collect information from a user during the login process, compare the information to a migration list to determine if the user is selected for migration and migrate the user transparently from the existing authentication system to the new authentication system.

[0009] The illustrative aspects of the present invention are designed to solve the problems herein described and other problems not discussed.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] These and other features of this invention will be more readily understood from the following detailed description of the various aspects of the invention taken in conjunction with the accompanying drawings.

[0011] FIG. **1** depicts a computer system having a migration system in accordance with an embodiment of the present invention.

[0012] FIG. **2** illustrates an example of a migration list.

[0013] FIG. **3** depicts a flow diagram of embodiments of a method of using the system of FIG.

[0014] The drawings are merely schematic representations, not intended to portray specific parameters of the invention. The drawings are intended to depict only typical embodiments of the invention, and therefore should not be considered as limiting the scope of the invention. In the drawings, like numbering represents like elements.

DETAILED DESCRIPTION OF THE INVENTION

[0015] Referring to FIG. **1**, a computer system **100** for migrating users from an existing authentication system **122** to a new authentication system **124** is shown, and generally includes a processor **104**, a bus **106**, an input/output (I/O) **108** and a memory **110**. Stored in memory **110** is a migration system **112** that includes a login system **114** that collects credential information from a user **102** (e.g., user identification and password) to allow access to secure resource **128**, a migration list check system **116** that compares the information of user **102** to a migration list **126**, and a migration logic system **118** that migrates user **102** from the existing authentication system **122** to the new authentication system **124** (if selected). Secure resource **128** may include, as an example, a bank account, retirement account or history of mortgage payments. In one embodiment, user **102** may be able to access one or more secure resources **128** through new authentication system **124**.

[0016] Login system **114** may comprise any system for collecting user credentials to authenticate user **102**. For

example, login system **114** may collect a user identification, password, voice recognition, or biometric data such as fingerprints, retinal scans, etc.

[0017] Migration list check system **116** utilizes migration list **126** to identify the users to be migrated from existing authentication system **122** to new authentication system **124**. Initially, user **102** enters their credentials into login system **114**. Login system **114** then checks for the existence of user **102** in new authentication system **124**. If user **102** is in new authentication system **124**, then login system **114** logs user **102** in new authentication system **124**. If user **102** is not in new authentication system **124**, then migration list check system **116** checks migration list **126** to determine if user **102** has been selected for migration. If user **102** is not selected for migration, migration list check system **116** causes user **102** to be logged in using existing authentication system **122**. If user **102** is selected for migration, then migration logic system **118** migrates user **102** from existing authentication system **122** to new authentication system **124** as part of the login process.

[0018] Migration system **112** may migrate user **102** selectively from existing authentication system **122** to new authentication system **124** to, for example, allow for a phased migration. In an illustrative embodiment, migration list **126** contains a list of users that have been selected for migration. The selection of the users for migration may be based on any number of criteria. For example, the users selected for migration may be determined on a specific class of users, on frequency of use of the secure resource **128**, or the size of the user's account, to name a few. In selecting users for migration, migration system **112** may use one of these or another criterion. Migration system **112** migrates user **102** from existing authentication system **122** to new authentication system **124** at the next time user **102** logs into login system **114** after being "selected" (i.e., selected for migration in migration list **126**).

[0019] The phased migration of users may result in a conservation of resources for computer system **100** as the migration occurs over time compared to the migration occurring all at once. Additionally, the phased migration may allow for the migration's progression to be observed and, if necessary, for changes to be made during the migration. Phased migration may also allow for changing during migration which users are to be migrated, the speed of migration and if an additional new secure resource **128** should be included or one removed.

[0020] In one embodiment, migration logic system **118** can perform the migration using a web authentication system. In an alternative embodiment, the migration can be architected to run in any environment where migration across authentication systems is needed. When migration utilizes a web authentication system, a migration website may be installed between existing authentication system **122** and user **102**. This can be done, for example, by changing the domain name system (DNS) address of the authentication domain to point to the migration server.

[0021] When a user is selected for migration, migration logic system **118** captures a user's password during login and automatically stores the password in new authentication system **124** upon a successful authentication in existing authentication system **122**. In another embodiment, the expiration date of user's password is also migrated from existing authentication system **122** to new authentication system **124**. The migration of user **102** from existing authentication system **122** to new authentication system **124** may be transparent to user **102**. Thus, user **102**, when being migrated from existing authentication system **122** to new authentication system **124**, will not know they are being migrated.

[0022] It is understood that computer system **100** may be implemented as any type of computing infrastructure. The processor **104** may comprise a single processing unit, or be distributed across one or more processing units in one or more locations (e.g., on a client and server). Memory **110** may comprise any known type of data storage, including magnetic media, optical media, random access memory (RAM), read-only memory (ROM), a data cache, a data object, etc. Moreover, memory **110** may reside at a single physical location, comprising one or more types of data storage, or be distributed across a plurality of physical systems in various forms.

[0023] I/O **108** may comprise any system for exchanging information to/from an external resource. External devices/resources may comprise any known type of external device, including a monitor/display, speakers, storage, another computer system, a hand-held device, keyboard, mouse, voice recognition system, speech output system, printer, facsimile, pager, etc. Bus **106** provides a communication link between each of the components in computer system **100** and likewise may comprise any known type of transmission link, including electrical, optical, wireless, etc. Although not shown, additional components, such as cache memory, communication systems, system software, etc., may be incorporated into computer system **100**.

[0024] Access to computer system **100** may be provided over a network such as the Internet, a local area network (LAN), a wide area network (WAN), a virtual private network (VPN), etc. Communication could occur via a direct hard-wired connection (e.g., serial port), or via an addressable connection that may utilize any combination of wireline and/or wireless transmission methods. Moreover, conventional network connectivity, such as Token Ring, Ethernet, WiFi or other conventional communications standards could be used. Still yet, connectivity could be provided by conventional TCP/IP sockets-based protocol. In this instance, an Internet service provider could be used to establish interconnectivity. Further, as indicated above, communication could occur in a client-server or server-server environment.

[0025] FIG. **2** illustrates a simple example of a migration list **126**. In this case, migration list **126** may include a list of all the users and the status of their migration (i.e., migration complete or migration not complete). Additionally, migration list **126** may include a date after which a user is to be migrated. For instance, migration list **126** may have a group of users set for migration after January 1st. The next time the users login after the pre-determined date (in this case, January 1st), the user will be migrated. Migration list **126** may include additional information regarding each user. For example, migration list **126** may include a user type, list the secure resource **128** (FIG. **1**) that is associated with user and provide the last time the user logged into the secure resource. The user type may also be used by the migration system to determine when users are to be selectively migrated.

[0026] FIG. **3** shows a flow diagram illustrating one embodiment of the process of migration system **112** (with reference to FIG. **1**). In process P**1**, user **102** enters their login information. In process P**2**, login system **114** checks for the existence of user **102** in new authentication system **124**. If user **102** is in new authentication system **124** (i.e., YES at P**2**), then login system **114** logs user **102** in new authentication system **124** (P**5**). If user **102** is not in new authentication system **124** (i.e., NO at process P**2**), then migration list check

system **116** checks if user **102** has been selected for migration (P**3**). Migration list check system **116** checks if user **102** is selected for migration by comparing user **102** to migration list **126**. If user **102** is not selected for migration (i.e., NO at process P**3**), then user **102** logs into existing authentication system **122**, process P**3**A. If user **102** is selected for migration (i.e., YES at process P**3**), then in process P**4** the user is migrated from existing authentication system **122** to new authentication system **124** using migration logic system **118**. In process P**5**, user **102** logs into and is authenticated by new authentication system **124**. Once user **102** is migrated from existing authentication system **122** to new authentication system **124**, migration list **126** is updated to indicate that user **102** was migrated to new authentication system **124**.

[0027] It should be appreciated that the teachings of the present invention could be offered as a business method on a subscription or fee basis. For example, a computer system **100** including memory **110** with migration system **112** could be created, maintained and/or deployed by a service provider that offers the functions described herein for customers. That is, a service provider could offer to deploy or provide a migration system **112** as described above.

[0028] It is understood that in addition to being implemented as a system and method, the features may be provided as a program product stored on a computer-readable medium, which when executed, enables computer system **100** to provide a migration system **112**. To this extent, the computer-readable medium may include program code, which implements the processes and systems described herein. It is understood that the term "computer-readable medium" comprises one or more of any type of physical embodiment of the program code. In particular, the computer-readable medium can comprise program code embodied on one or more portable storage articles of manufacture (e.g., a compact disc, a magnetic disk, a tape, etc.), on one or more data storage portions of a computing device, such as memory **110** and/or a storage system.

[0029] As used herein, it is understood that the terms "program code" and "computer program code" are synonymous and mean any expression, in any language, code or notation, of a set of instructions that cause a computing device having an information processing capability to perform a particular function either directly or after any combination of the following: (a) conversion to another language, code or notation; (b) reproduction in a different material form; and/or (c) decompression. To this extent, program code can be embodied as one or more types of program products, such as an application/software program, component software/a library of functions, an operating system, a basic I/O system/driver for a particular computing and/or I/O device, and the like. Further, it is understood that terms such as "component" and "system" are synonymous as used herein and represent any combination of hardware and/or software capable of performing some function(s).

[0030] The block diagrams in the figures illustrate the architecture, functionality, and operation of possible implementations of systems, methods and computer program products according to various embodiments of the present invention. In this regard, each block in the block diagrams may represent a module, segment, or portion of code, which comprises one or more executable instructions for implementing the specified logical function(s). It should also be noted that the functions noted in the blocks may occur out of the order noted in the figures. For example, two blocks shown in succession may, in fact, be executed substantially concurrently, or the blocks may sometimes be executed in the reverse order, depending upon the functionality involved. It will also be noted that each block of the block diagrams can be implemented by special purpose hardware-based systems which perform the specified functions or acts, or combinations of special purpose hardware and computer instructions.

[0031] Although specific embodiments have been illustrated and described herein, those of ordinary skill in the art appreciate that any arrangement which is calculated to achieve the same purpose may be substituted for the specific embodiments shown and that the invention has other applications in other environments. This application is intended to cover any adaptations or variations of the present invention. The following claims are in no way intended to limit the scope of the invention to the specific embodiments described herein.

What is claimed is:

1. A system for migrating a user from an existing authentication system to a new authentication system, comprising:
- a login system that collects information from the user during a login process;
- a migration list check system that compares the information to a migration list to determine if the user is selected for migration; and
- a migration logic system that migrates the user from the existing authentication system to the new authentication system during the login process if the user is selected.

2. The system of claim **1**, wherein the migration list identifies a set of users to be migrated.

3. The system of claim **1**, wherein the migration system migrates the user selectively from the existing authentication system to the new authentication system.

4. The system of claim **1**, wherein the migration system migrates the user from the existing authentication system to the new authentication system a first time the user logs in after being selected.

5. The system of claim **1**, wherein a password is captured during the login process and automatically stored in the new authentication system when the user is migrated.

6. The system of claim **5**, wherein an expiration of the password is migrated from the existing authentication system to the new authentication system.

7. The system of claim **1**, wherein the migration of the user from the existing authentication system to the new authentication system is transparent to the user.

8. A computer readable medium having a program product stored therein for migrating a user from an existing authentication system to a new authentication system, comprising:
- program code that collects information from the user during a login process;
- program code that compares the information to a migration list to determine if the user is selected for migration; and
- program code that migrates the user from the existing authentication system to the new authentication system during the login process if the user is selected.

9. The computer readable medium of claim **8**, wherein the migration list identifies a set of users to be migrated.

10. The computer readable medium of claim **8**, further comprising program code for migrating the user selectively from the existing authentication system to the new authentication system.

11. The computer readable medium of claim **8**, further comprising program code for migrating the user from the

existing authentication system to the new authentication system a first time the user logs in after being selected.

12. The computer readable medium of claim **8**, further comprising program code for capturing a password during the login process and automatically storing the password in the new authentication system when the user is migrated.

13. The computer readable medium of claim **12**, further comprising program code for migrating the expiration date of the password from the existing authentication system to the new authentication system.

14. The computer readable medium of claim **8**, wherein the migration of the user from the existing authentication system to the new authentication system is transparent to the user.

15. A method of migrating a user from an existing authentication system to a new authentication system, comprising:

collecting information from the user during a login process of a computer system;

comparing the information to a migration list to determine if the user is selected for migration; and

migrating the user from the existing authentication system to the new authentication system during the login process if the user is selected.

16. The method of claim **15**, wherein the migration list identifies a set of users to be migrated.

17. The method of claim **15**, wherein the migration of the user occurs selectively from the existing authentication system to the new authentication system.

18. The method of claim **15**, wherein the migration of the user from the existing authentication system to the new authentication system occurs a first time the user logs in after being selected.

19. The method of claim **15**, wherein a password is captured during the login process and automatically stored in the new authentication system when the user is migrated.

20. A method for deploying a system for migrating a user from an existing authentication system to a new authentication system, comprising:

providing a computer infrastructure being operable to:

collect information from a user during a login process;

compare the information to a migration list to determine if the user is selected for migration;

select the user for migration from the existing authentication system to the new authentication system; and

migrate the user transparently from the existing authentication system to the new authentication system.

* * * * *

9.10 MOBILE DEVICE PASSWORD RESET


US009078135B2

(12) **United States Patent**
Bravo et al.

(10) **Patent No.: US 9,078,135 B2**
(45) **Date of Patent: Jul. 7, 2015**

(54) **MOBILE DEVICE PASSWORD RESET**

(71) Applicant: **International Business Machines Corporation**, Armonk, NY (US)

(72) Inventors: **Jose F. Bravo**, Mamaroneck, NY (US); **Jeffery L. Crume**, Raleigh, NC (US); **Nigel C. P. Hinds**, Upper Nyack, NY (US)

(73) Assignee: **International Business Machines Corporation**, Armonk, NY (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 21 days.

(21) Appl. No.: **14/020,937**

(22) Filed: **Sep. 9, 2013**

(65) **Prior Publication Data**

US 2015/0072646 A1 Mar. 12, 2015

(51) **Int. Cl.**
H04W 12/08 (2009.01)
H04L 29/06 (2006.01)

(52) **U.S. Cl.**
CPC ***H04W 12/08*** (2013.01); ***H04L 63/06*** (2013.01)

(58) **Field of Classification Search**
CPC H04W 12/06; H04W 63/08; H04W 12/12; H04W 12/08; H04M 1/67; H04M 1/673; H04M 3/42314
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2003/0088633	A1 *	5/2003	Chiu et al.	709/206
2011/0159844	A1	6/2011	Gillet et al.	
2014/0085048	A1 *	3/2014	Hadizad	340/5.64
2014/0113593	A1 *	4/2014	Zhou et al.	455/411

OTHER PUBLICATIONS

Unknown, "Automatic Mobile Phone Unlock Beyond a Predetermined Call Duration Threshold of a Trusted Call", IP.com Prior Art Database Technical Disclosure, IPCOM000224591D, Jan. 2, 2013, 2 pages.
Notice of Allowance and Fee(s) Due for U.S. Appl. No. 14/079,705, dated April 27, 2015, 18 pages.

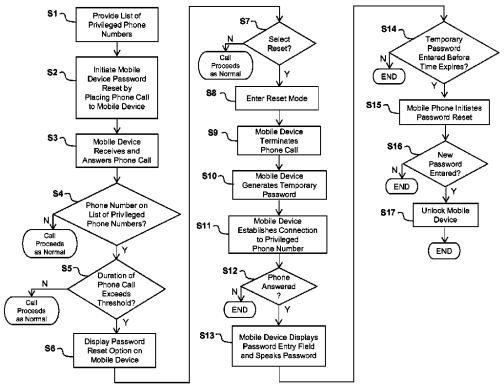
* cited by examiner

Primary Examiner — Kamran Afshar
Assistant Examiner — Ather Mohiuddin
(74) *Attorney, Agent, or Firm* — Andrea Barbuto; Hoffman Warnick LLC

(57) **ABSTRACT**

The disclosure is directed to a mobile device password reset. A method in accordance with an embodiment includes: receiving a phone call at a locked mobile device from a phone having a privileged phone number; initiating a password reset in response to the receipt of the phone call from the privileged phone number and the phone call exceeding a predetermined time duration threshold by: terminating, by the locked mobile device, the phone call from the phone having the privileged phone number; generating, by the locked mobile device, a temporary password; establishing, by the locked mobile device, a connection to the phone having the privileged phone number; displaying, by the locked mobile device, a password entry field; communicating, by the locked mobile device, the temporary password via the connection to the phone having the privileged phone number; and unlocking the locked mobile device upon successful entry of the temporary password in the password entry field displayed by the locked mobile device.

20 Claims, 6 Drawing Sheets



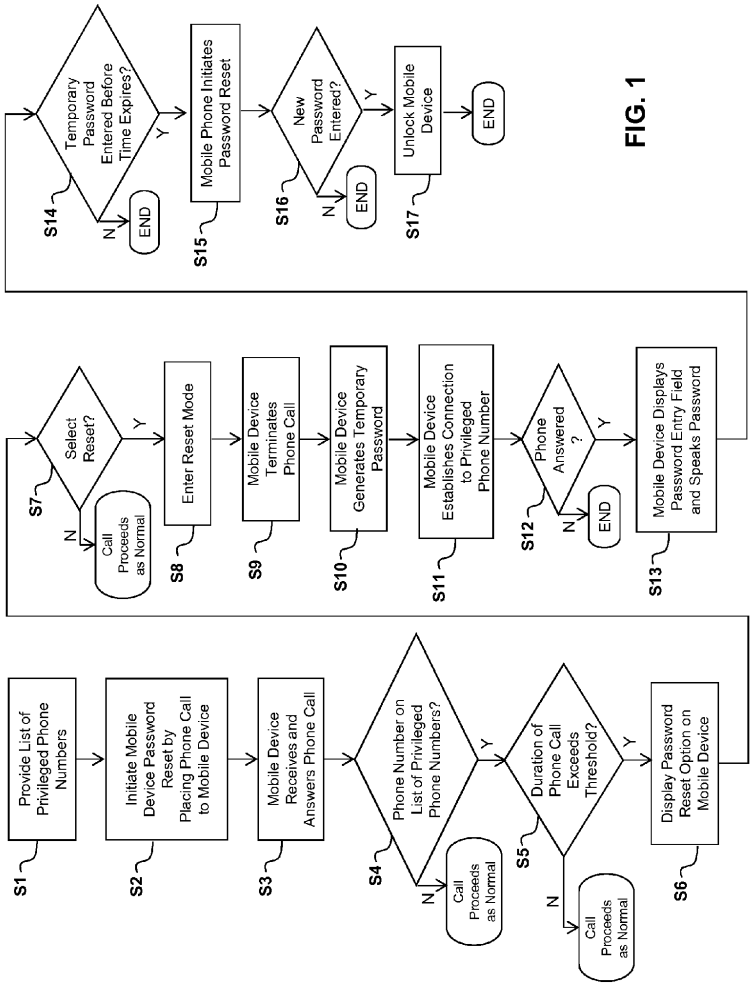

Provide List of Privileged Phone Numbers
S1
Initiate Mobile Device Password Reset by Placing Phone Call to Mobile Device
S2
Mobile Device Receives and Answers Phone Call
S3
Phone Number on List of Privileged Phone Numbers?
S4
Y
N
Call Proceeds as Normal
Duration of Phone Call Exceeds Threshold?
S5
Y
N
Call Proceeds as Normal
Display Password Reset Option on Mobile Device
S6
Select Reset?
S7
Y
N
Call Proceeds as Normal
Enter Reset Mode
S8
Mobile Device Terminates Phone Call
S9
Mobile Device Generates Temporary Password
S10
Mobile Device Establishes Connection to Privileged Phone Number
S11
Phone Answered ?
S12
Y
N
END
Mobile Device Displays Password Entry Field and Speaks Password
S13
Temporary Password Entered Before Time Expires?
S14
Y
N
END
Mobile Phone Initiates Password Reset
S15
New Password Entered?
S16
Y
N
END
Unlock Mobile Device
S17
END

FIG. 1

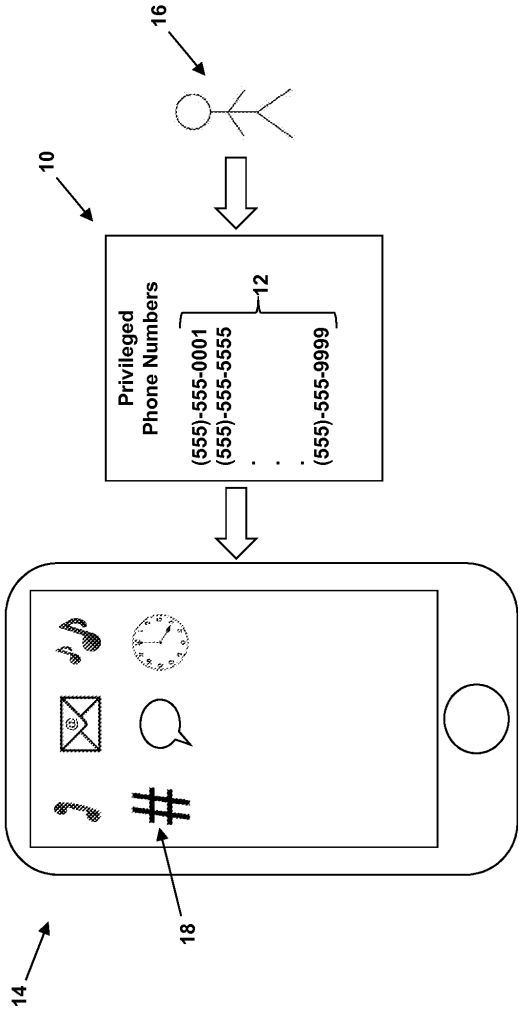

16
10
Privileged
Phone Numbers
12
(555)-555-0001
(555)-555-5555
. . .
(555)-555-9999
18
14

FIG. 2

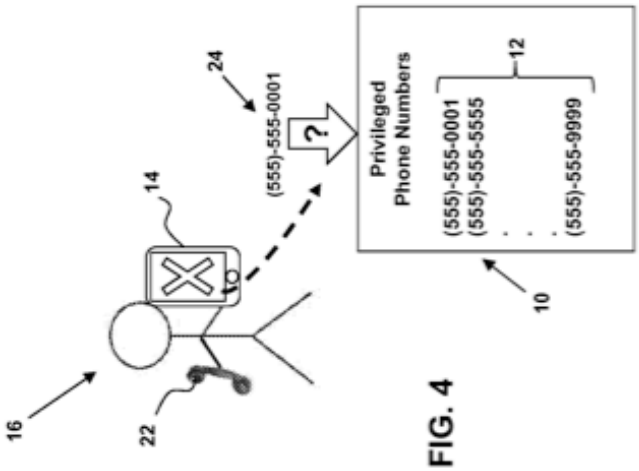

24
(555)-555-0001
?
Privileged
Phone Numbers
12
(555)-555-0001
(555)-555-5555
(555)-555-9999
14
16
22
10

FIG. 4

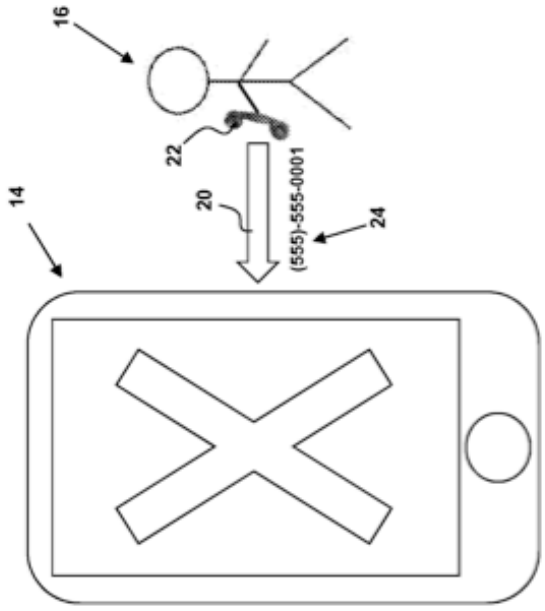

16
22
20
(555)-555-0001
24
14

FIG. 3

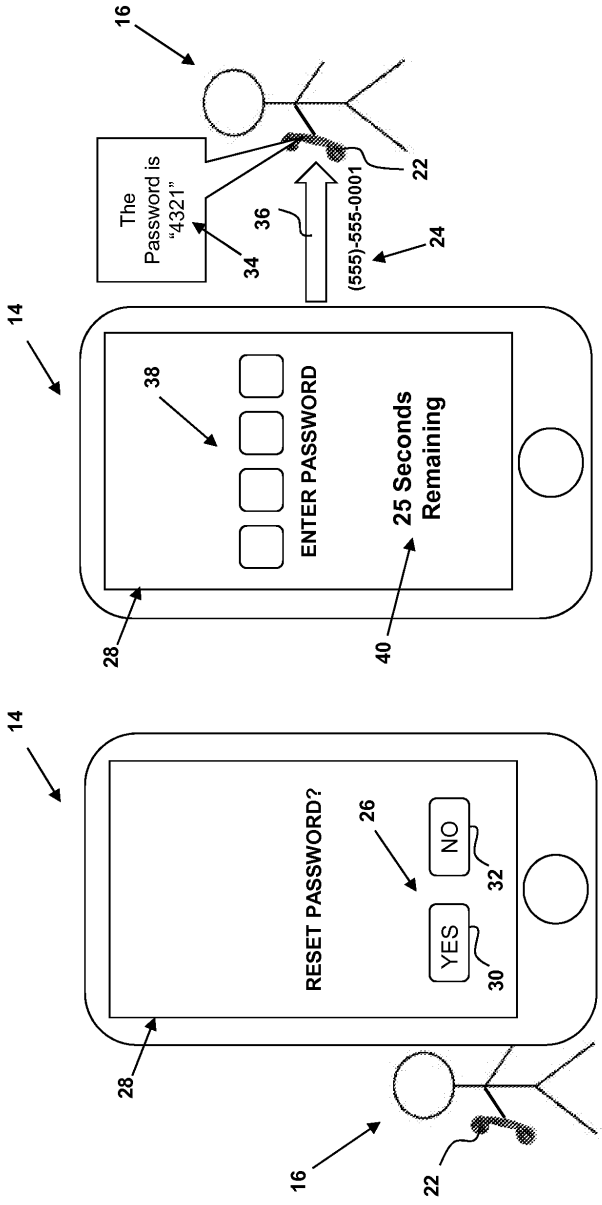

16
The Password is "4321"
34
36
(555)-555-0001
24
22
14
38
ENTER PASSWORD
25 Seconds Remaining
28
40

FIG. 6

14
RESET PASSWORD?
26
NO
32
YES
30
28
16
22

FIG. 5

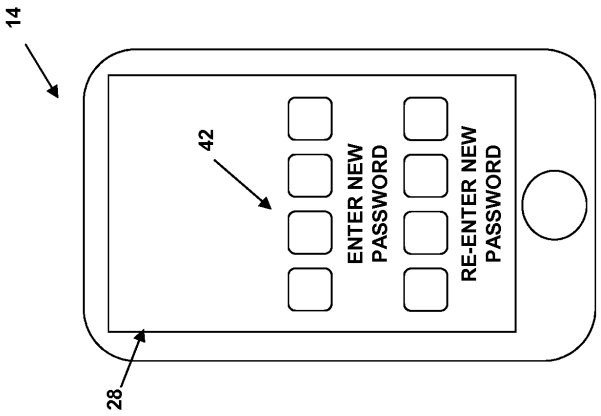


FIG. 7

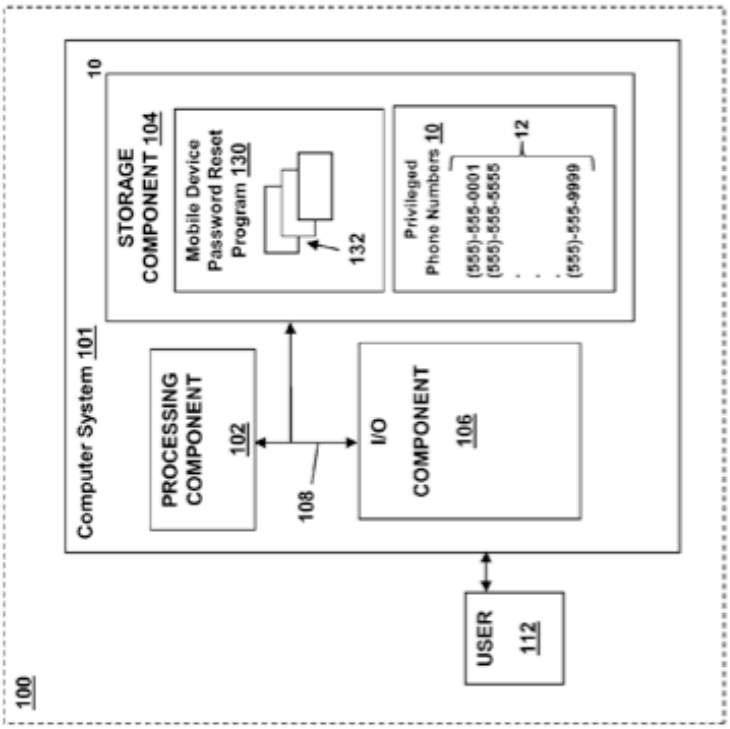

100
Computer System 101
10
STORAGE COMPONENT 104
Mobile Device Password Reset Program 130
132
Privileged Phone Numbers 10
12
(555)-555-0001
(555)-555-5555
(555)-555-9999
PROCESSING COMPONENT 102
108
I/O COMPONENT 106
USER 112

FIG. 8

MOBILE DEVICE PASSWORD RESET

TECHNICAL FIELD

The present invention relates generally to mobile devices, and more particularly, to a mobile device password reset.

RELATED ART

Many methods are available for resetting a forgotten or lost password of a mobile device. One method, typically referred to as a master or factory reset, returns a mobile device to its original, default operating system state. However, this process erases all data (e.g., contacts, applications, personalized settings, etc.) added to the mobile device after purchase. Another method requires a phone call to the phone company that provides service to the mobile device. The present invention addresses these problems allowing users to avoid the data reconstruction of a hard reset and the cost of service provider involvement.

SUMMARY

A first aspect of the invention provides a mobile device password reset method, comprising: receiving a phone call at a locked mobile device from a phone having a privileged phone number; initiating a password reset in response to the receipt of the phone call from the phone having the privileged phone number and the phone call exceeding a predetermined time duration threshold, the password reset comprising: terminating, by the locked mobile device, the phone call from the privileged phone number; generating, by the locked mobile device, a temporary password; establishing, by the locked mobile device, a connection to the phone having the privileged phone number; displaying, by the locked mobile device, a password entry field; communicating, by the locked mobile device, the temporary password via the connection to the phone having the privileged phone number; and unlocking the locked mobile device upon successful entry of the temporary password in the password entry field displayed by the locked mobile device.

A second aspect of the invention provides a mobile device configured to perform a password reset method, the method comprising: receiving a phone call at a locked mobile device from a phone having a privileged phone number; initiating a password reset in response to the receipt of the phone call from the phone having the privileged phone number and the phone call exceeding a predetermined time duration threshold, the password reset comprising: terminating, by the locked mobile device, the phone call from the privileged phone number; generating, by the locked mobile device, a temporary password; establishing, by the locked mobile device, a connection to the phone having the privileged phone number; displaying, by the locked mobile device, a password entry field; communicating, by the locked mobile device, the temporary password via the connection to the phone having the privileged phone number; and unlocking the locked mobile device upon successful entry of the temporary password in the password entry field displayed by the locked mobile device.

A third aspect of the invention provides a computer program product including program code embodied in at least one computer-readable storage medium, which when executed, enables a computer system to implement a mobile device password reset method, the method comprising: receiving a phone call at a locked mobile device from a phone having a privileged phone number; initiating a password reset in response to the receipt of the phone call from the phone having the privileged phone number and the phone call exceeding a predetermined time duration threshold, the password reset comprising: terminating, by the locked mobile device, the phone call from the privileged phone number; generating, by the locked mobile device, a temporary password; establishing, by the locked mobile device, a connection to the phone having the privileged phone number; displaying, by the locked mobile device, a password entry field; communicating, by the locked mobile device, the temporary password via the connection to the phone having the privileged phone number; and unlocking the locked mobile device upon successful entry of the temporary password in the password entry field displayed by the locked mobile device.

Other aspects of the invention provide methods, systems, program products, and methods of using and generating each, which include and/or implement some or all of the actions described herein. The illustrative aspects of the invention are designed to solve one or more of the problems herein described and/or one or more other problems not discussed.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other features of the disclosure will be more readily understood from the following detailed description of the various aspects of the invention taken in conjunction with the accompanying drawings that depict various aspects of the invention.

FIG. **1** shows a flow diagram of an illustrative process for a mobile device password reset, according to embodiments.

FIG. **2** depicts an illustrative setup process for a mobile device password reset, according to embodiments.

FIG. **3** depicts a user initiating a mobile device password reset by placing a phone call to a locked mobile device, according to embodiments.

FIG. **4** depicts a locked mobile device comparing the phone number of a received phone call to privileged phone numbers on a predefined list, according to embodiments.

FIG. **5** depicts the display of a password reset option to a user via a display of a mobile device, according to embodiments.

FIG. **6** depicts a mobile device placing a return phone call to the phone number of the phone that initiated a mobile device password reset, according to embodiments.

FIG. **7** depicts the initiation of a password reset upon receiving a correct temporary password, according to embodiments.

FIG. **8** shows an illustrative environment for a mobile device password reset according to an embodiment.

It is noted that the drawings may not be to scale. The drawings are intended to depict only typical aspects of the invention, and therefore should not be considered as limiting the scope of the invention. In the drawings, like numbering represents like elements between the drawings.

DETAILED DESCRIPTION

The present invention relates generally to mobile devices, and more particularly, to a mobile device password reset.

When a mobile device enters a locked state, operation of the mobile device may be prevented or severely limited. Such a locked state may occur automatically, for example, after a predetermined period of inactivity, or may be activated manually (e.g., via buttons/keys on the mobile device or remotely over the Internet). Typically, the locked state of a mobile device is provided as a security measure to prevent unauthorized or unintended use of the mobile device. However, while

in the locked state, most mobile devices allow incoming phone calls, which can be answered by a user of the mobile device, and/or a user of the mobile device may be able to place an outgoing emergency call.

To unlock a mobile device that has entered a locked state, a user typically enters a password into a password entry screen of the mobile device using a virtual or physical keypad of the mobile device. A password may comprise, for example, an alphanumeric passcode, passkey, passphrase, access code, personal identification number (PIN), a pattern entered on the screen, or other type of authentication data. If the user correctly enters the password within a predetermined number of attempts, the mobile device is unlocked and full functionality is restored. Repeated failures to enter the correct password may, in some cases, cause the mobile device to erase all data and perform a master reset.

The present invention provides a mobile device password reset that allows a user to securely regain full authorized access to a locked mobile device. In the present disclosure, such a mobile device may include, for example, a cell phone, smartphone, tablet computer, PDA, laptop computer, or other handheld computing/communication device capable of sending/receiving phone calls.

FIG. **1** shows a flow diagram of an illustrative process for a mobile device password reset according to embodiments. During a setup process S**1**, and as depicted in FIG. **2**, a predefined list **10** of one or more privileged phone numbers **12** is provided and stored in a mobile device **14** by an authorized user **16** (e.g., owner) of the mobile device **14**. For example, the predefined list **10** of privileged phone numbers **12** may include the home and work phone numbers of the user **16**, a friend's cell phone number, a relative's land-line phone number, etc.

The user **16** may provide the predefined list **10** of privileged phone numbers **12** during an initial or subsequent configuration of the settings of the mobile device **14**. Application software **18** loaded and running on the mobile device **14** may also be used to provide the predefined list **10** of privileged phone numbers **12** to the mobile device **14**.

At S**2**, assuming the mobile device **14** is in a locked state and the user **16** has forgotten the password for unlocking the mobile device **14**, the user **16** initiates a mobile device password reset by placing a phone call **20** (FIG. **3**) to the mobile device **14** from another phone **22**. The phone **22** can comprise any telecommunication device capable of sending/receiving phone calls, including a mobile device, a land-line phone, a computer with VoIP capabilities, and/or the like. At S**3**, the phone call **20** is received and answered by the mobile device **14**.

At S**4**, the mobile device **14** compares (FIG. **4**) the phone number **24** of the phone call **20** to the privileged phone numbers **12** on the predefined list **10**. The phone number **24** of the phone call **20** may be determined via caller ID or using any other suitable technique.

If the phone number **24** of the phone call **20** is not on the predefined list **10** of privileged phone numbers **12** (N at S**4**), the mobile device password reset process ends and the call proceeds as normal. If, however, the phone number **24** of the phone call **20** is on the predefined list **10** of privileged phone numbers **12** (Y at S**4**), flow passes to S**5**.

At S**5**, the elapsed duration of the phone call **20** is monitored by the mobile device **14**. If the elapsed duration of the phone call **20** exceeds a predetermined time threshold (e.g., 10-15 seconds) (Y at S**5**), indicating that the phone call **20** has a high likelihood of being legitimate, a password reset option **26** (FIG. **5**) is displayed to the user **16** at S**6** via a display **28** of the mobile device **14**. If the phone call **20** is terminated before the predetermined time threshold has been exceeded (N at S**5**), the mobile device password reset process ends and the call proceeds as normal. The duration of the phone call **20** will generally be shorter in the case that the mobile device **14** is lost/stolen. In such a case, the user **16** would realize the mobile device **14** has been compromised (e.g., based on who answered the mobile device **14**) and hang-up before the predetermined time threshold, thereby terminating the mobile device password reset process.

If the user **16** selects the password reset option **26** (Y at S**7**), the mobile device **14** enters a password reset mode at S**8**. If the user **16** does not select the password reset option **26** (N at S**7**), the mobile device password reset process ends and the call proceeds as normal. Selection of the password reset option **26** may be provided, for example, via YES and NO buttons **30**, **32**, respectively, or in any other suitable manner.

Upon entering the password reset mode at S**8**, the mobile device **14** terminates the phone call **20** at S**9**. Thereafter, at S**10**, the mobile device **14** generates a random, one-time, temporary password **34** (FIG. **6**).

At S**11**, and as shown in FIG. **6**, the mobile device **14** establishes a connection (e.g., via a return phone call **36**) to the phone number **24** of the phone **22** that initiated the mobile device password reset. If the return phone call **36** is not answered by the user **16** (N at S**12**) the mobile device password reset process ends. If the return phone call **36** is answered by the user **16** (Y at S**12**), the mobile device **14**, at S**13**, displays a password entry field **38** and speaks the temporary password **34** to the user **16** (e.g., using text-to-speech) one or more times for a predetermined period of time (e.g., 30 seconds). In other embodiments, the mobile device **14** may communicate the temporary password **34** to the user **16** in a non-vocal manner. For example, the mobile device **14** may communicate the temporary password **34** to the user **16** via a short message service (SMS) text message, an email, and/or the like.

If the user **16** does not enter the correct temporary password **34** into the displayed password entry field **38** within the predetermined period of time (N at S**14**), the mobile device password reset process ends. If the user **16** enters the correct temporary password **34** into the displayed password entry field **38** within the predetermined period of time (Y at S**14**), flow passes to S**15**. As depicted in FIG. **6**, a timer **40** may be displayed on the mobile device **14** to indicate the time remaining during which the user **16** can enter the correct temporary password **34** into the displayed password entry field **38**.

At S**15**, upon receiving the correct temporary password **34**, the mobile device **14** immediately initiates a password change process (FIG. **7**), after which the user **16** is required to enter a new password **42** into the mobile device **14**. After successful completion of the password change process (Y at S**16**), the mobile device **14** is unlocked at S**17** and is ready for use. If the password reset is not completed (N at S**16**), the mobile device **14** remains locked and the mobile device password reset process ends. In this case, the user **16** must return to S**2** to restart the mobile device password reset process.

An illustrative environment **100** for providing a mobile device password reset is shown in FIG. **8**. The environment **100** includes at least one computer system **101** and a mobile device password reset program **130** that can perform processes described herein in order to provide a mobile device password reset in accordance with embodiments. The environment **100** may be provided, for example, within a mobile device **14**.

The computer system **101** is shown including a processing component **102** (e.g., one or more processors), a storage component **104** (e.g., a storage hierarchy), an input/output

(I/O) component **106** (e.g., one or more I/O interfaces and/or devices), and a communications pathway **108**. In general, the processing component **102** executes program code, such as the mobile device password reset program **130**, which is at least partially fixed in the storage component **104**. While executing program code, the processing component **102** can process data, such as a list **10** of privileged phone numbers **12** and/or the like, which can result in reading and/or writing transformed data from/to the storage component **104** and/or the I/O component **106** for further processing. The pathway **108** provides a communications link between each of the components in the computer system **101**. The I/O component **106** can include one or more human I/O devices, which enable a human user **112** to interact with the computer system **101** and/or one or more communications devices to enable a system user **112** to communicate with the computer system **101** using any type of communications link. To this extent, the mobile device password reset program **130** can manage a set of interfaces (e.g., graphical user interface(s), application program interfaces, communication interface(s), and/or the like) that enable human and/or system users **112** to interact with the mobile device password reset program **130**. Furthermore, the mobile device password reset program **130** can manage (e.g., store, retrieve, create, manipulate, organize, present, etc.) the data, such as the list **10** of privileged phone numbers **12** and/or the like, using any solution.

The computer system **101** can include one or more general purpose computing articles of manufacture (e.g., computing devices) capable of executing program code, such as the mobile device password reset program **130**, installed thereon. As used herein, it is understood that "program code" means any collection of instructions, in any language, code or notation, that cause a computing device having an information processing capability to perform a particular action either directly or after any combination of the following: (a) conversion to another language, code or notation; (b) reproduction in a different material form; and/or (c) decompression. To this extent, the mobile device password reset program **130** can be embodied as any combination of system software and/or application software.

Furthermore, the mobile device password reset program **130** can be implemented using a set of modules **132**. In this case, a module **132** can enable the computer system **20** to perform a set of tasks used by the mobile device password reset program **130**, and can be separately developed and/or implemented apart from other portions of the mobile device password reset program **130**. As used herein, the term "component" means any configuration of hardware, with or without software, which implements the functionality described in conjunction therewith using any solution, while the term "module" means program code that enables a computer system **101** to implement the actions described in conjunction therewith using any solution. When fixed in a storage component **104** of a computer system **101** that includes a processing component **102**, a module is a portion of a component that implements the actions. Regardless, it is understood that two or more components, modules, and/or systems may share some/all of their respective hardware and/or software. Furthermore, it is understood that some of the functionality discussed herein may not be implemented or additional functionality may be included as part of the computer system **101**.

When the computer system **101** includes multiple computing devices, each computing device can have only a portion of the mobile device password reset program **130** fixed thereon (e.g., one or more modules **132**). However, it is understood that the computer system **101** and the mobile device password reset program **130** are only representative of various possible equivalent computer systems that may perform a process described herein. To this extent, in other embodiments, the functionality provided by the computer system **101** and the mobile device password reset program **130** can be at least partially implemented by one or more computing devices that include any combination of general and/or specific purpose hardware with or without program code. In each embodiment, the hardware and program code, if included, can be created using standard engineering and programming techniques, respectively.

When the computer system **101** includes multiple computing devices, the computing devices can communicate over any type of communications link. Furthermore, while performing a process described herein, the computer system **101** can communicate with one or more other computer systems using any type of communications link. In either case, the communications link can include any combination of various types of optical fiber, wired, and/or wireless links; include any combination of one or more types of networks; and/or utilize any combination of various types of transmission techniques and protocols.

While shown and described herein as a method and system for detecting illegal activity through interpersonal relationship resolution, it is understood that aspects of the invention further provide various alternative embodiments. For example, in one embodiment, the invention provides a computer program fixed in at least one computer-readable storage medium, which when executed, enables a computer system to for detect illegal activity through interpersonal relationship resolution. To this extent, the computer-readable storage medium includes program code, such as the mobile device password reset program **130**, which enables a computer system to implement some or all of a process described herein. It is understood that the term "computer-readable storage medium" includes one or more of any type of tangible medium of expression, now known or later developed, from which a copy of the program code can be perceived, reproduced, or otherwise communicated by a computing device. For example, the computer-readable medium can include: one or more portable storage articles of manufacture; one or more memory/storage components of a computing device; paper; and/or the like.

Another embodiment of the invention provides a method of providing a copy of program code, such as the mobile device password reset program **30**, which enables a computer system to implement some or all of a process described herein. In this case, a computer system can process a copy of the program code to generate and transmit, for reception at a second, distinct location, a set of data signals that has one or more of its characteristics set and/or changed in such a manner as to encode a copy of the program code in the set of data signals. Similarly, an embodiment of the invention provides a method of acquiring a copy of the program code, which includes a computer system receiving the set of data signals described herein, and translating the set of data signals into a copy of the computer program fixed in at least one computer-readable medium. In either case, the set of data signals can be transmitted/received using any type of communications link.

Still another embodiment of the invention provides a method for providing a mobile device password reset. In this case, a computer system, such as the computer system **101**, can be obtained (e.g., created, maintained, made available, etc.) and one or more components for performing process(es) described herein can be obtained (e.g., created, purchased, used, modified, etc.) and deployed to the computer system. To this extent, the deployment can include one or more of: (1) installing program code on a computing device; (2) adding

one or more computing and/or I/O devices to the computer system; (3) incorporating and/or modifying the computer system to enable it to perform a process described herein; and/or the like.

The foregoing description of various aspects of the invention has been presented for purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise form disclosed, and obviously, many modifications and variations are possible. Such modifications and variations that may be apparent to an individual skilled in the art are included within the scope of the invention as defined by the accompanying claims.

What is claimed is:

1. A mobile device password reset method, comprising:

receiving a phone call at a locked mobile device from a phone having a privileged phone number;

initiating a password reset in response to the receipt of the phone call from the phone having the privileged phone number and the phone call exceeding a predetermined time duration threshold, the password reset comprising:

terminating, by the locked mobile device, the phone call from the privileged phone number;

generating, by the locked mobile device, a temporary password;

establishing, by the locked mobile device, a connection to the phone having the privileged phone number;

displaying, by the locked mobile device, a password entry field;

communicating, by the locked mobile device, the temporary password via the connection to the phone having the privileged phone number; and

unlocking the locked mobile device upon successful entry of the temporary password in the password entry field displayed by the locked mobile device.

2. The mobile device password reset method of claim **1**, wherein the connection comprises a phone call.

3. The mobile device password reset method of claim **1**, wherein the connection comprises a text message.

4. The mobile device password reset method according to claim **1**, wherein the unlocking further comprises:

initiating, by the mobile device, a timer when communicating the temporary password via the connection to the phone having the privileged phone number; and

unlocking the locked mobile device upon successful entry of the temporary password in the displayed password entry field within a predetermined period of time as determined via the timer.

5. The mobile device password reset method according to claim **1**, wherein the unlocking further comprises:

requesting, by the locked mobile device, a new password upon successful entry of the temporary password in the displayed password entry field; and

unlocking the locked mobile device upon successful entry of the new password.

6. The mobile device password reset method according to claim **1**, wherein the communicating further comprises:

speaking, by the locked mobile device, the temporary password during the connection.

7. The mobile device password reset method according to claim **1**, further comprising:

storing at least one privileged phone number in the mobile device.

8. The mobile device password reset method according to claim **7**, wherein

the initiating the password reset further comprises:

comparing a phone number of the received phone call to each of the privileged phone numbers stored in the mobile device; and

initiating the password reset when the phone number of the received phone call matches one of the privileged phone numbers stored in the mobile device.

9. A mobile device configured to perform a password reset method, the method comprising:

receiving a phone call at a locked mobile device from a phone having a privileged phone number;

initiating a password reset in response to the receipt of the phone call from the phone having the privileged phone number and the phone call exceeding a predetermined time duration threshold, the password reset comprising:

terminating, by the locked mobile device, the phone call from the privileged phone number;

generating, by the locked mobile device, a temporary password;

establishing, by the locked mobile device, a connection to the phone having the privileged phone number;

displaying, by the locked mobile device, a password entry field;

communicating, by the locked mobile device, the temporary password via the connection to the phone having the privileged phone number; and

unlocking the locked mobile device upon successful entry of the temporary password in the password entry field displayed by the locked mobile device.

10. The mobile device of claim **9**, wherein the connection comprises a phone call.

11. The mobile device of claim **9**, wherein the connection comprises a text message.

12. The mobile device according to claim **9**, wherein the unlocking further comprises:

initiating, by the mobile device, a timer when communicating the temporary password via the connection to the phone having the privileged phone number; and

unlocking the locked mobile device upon successful entry of the temporary password in the displayed password entry field within a predetermined period of time as determined via the timer.

13. The mobile device according to claim **9**, wherein the unlocking further comprises:

requesting, by the locked mobile device, a new password upon successful entry of the temporary password in the displayed password entry field; and

unlocking the locked mobile device upon successful entry of the new password.

14. The mobile device according to claim **9**, wherein the communicating further comprises:

speaking, by the locked mobile device, the temporary password during the connection.

15. The mobile device according to claim **9**, the method further comprising:

storing at least one privileged phone number in the mobile device.

16. The mobile device according to claim **15**, wherein the initiating the password reset further comprises:

comparing a phone number of the received phone call to each of the privileged phone numbers stored in the mobile device; and

initiating the password reset when the phone number of the received phone call matches one of the privileged phone numbers stored in the mobile device.

17. A computer program product comprising program code embodied in at least one non-transitory computer-readable

storage medium, which when executed, enables a computer system to implement a mobile device password reset method, the method comprising:

receiving a phone call at a locked mobile device from a phone having a privileged phone number;

initiating a password reset in response to the receipt of the phone call from the phone having the privileged phone number and the phone call exceeding a predetermined time duration threshold, the password reset comprising:

terminating, by the locked mobile device, the phone call from the privileged phone number;

generating, by the locked mobile device, a temporary password;

establishing, by the locked mobile device, a connection to the phone having the privileged phone number;

displaying, by the locked mobile device, a password entry field;

communicating, by the locked mobile device, the temporary password via the connection to the phone having the privileged phone number; and

unlocking the locked mobile device upon successful entry of the temporary password in the password entry field displayed by the locked mobile device.

18. The computer program product of claim **17**, wherein the connection comprises a phone call, a text message, or an email.

19. The computer program product of claim **17**, wherein the unlocking further comprises:

initiating, by the mobile device, a timer when communicating the temporary password via the connection to the phone having the privileged phone number; and

unlocking the locked mobile device upon successful entry of the temporary password in the displayed password entry field within a predetermined period of time as determined via the timer.

20. The computer program product of claim **17**, wherein the unlocking further comprises:

requesting, by the locked mobile device, a new password upon successful entry of the temporary password in the displayed password entry field; and

unlocking the locked mobile device upon successful entry of the new password.

* * * * *

US009088896B2

(12) **United States Patent**
Bravo et al.

(10) **Patent No.: US 9,088,896 B2**
(45) **Date of Patent: *Jul. 21, 2015**

(54) **MOBILE DEVICE PASSWORD RESET**

(71) Applicant: **International Business Machines Corporation**, Armonk, NY (US)

(72) Inventors: **Jose F. Bravo**, Mamaroneck, NY (US); **Jeffery L. Crume**, Raleigh, NC (US); **Nigel C. P. Hinds**, Upper Nyack, NY (US)

(73) Assignee: **International Business Machines Corporation**, Armonk, NY (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **14/079,705**

(22) Filed: **Nov. 14, 2013**

(65) **Prior Publication Data**

US 2015/0072648 A1 Mar. 12, 2015

Related U.S. Application Data

(63) Continuation of application No. 14/020,937, filed on Sep. 9, 2013.

(51) **Int. Cl.**
H04B 1/60 (2006.01)
H04B 7/15 (2006.01)
(Continued)

(52) **U.S. Cl.**
CPC ***H04W 12/08*** (2013.01); ***H04L 63/06*** (2013.01); ***H04L 63/083*** (2013.01)

(58) **Field of Classification Search**
CPC H04W 12/06; H04W 63/08; H04W 12/12; H04W 12/00; H04W 12/08; H04M 1/67; H04M 1/673; H04M 3/42314
USPC 455/10, 11, 414.1–420; 726/19, 1, 2, 3, 726/4; 340/571
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2003/0088633 A1* 5/2003 Chiu et al. 709/206
2011/0159844 A1 6/2011 Gillet et al.

(Continued)

OTHER PUBLICATIONS

Unknown, "Automatic Mobile Phone Unlock Beyond a Predetermined Call Duration Threshold of a Trusted Call", IP.com Prior Art Database Technical Disclosure, IPCOM000224591D, Jan. 2, 2013, 2 pages.

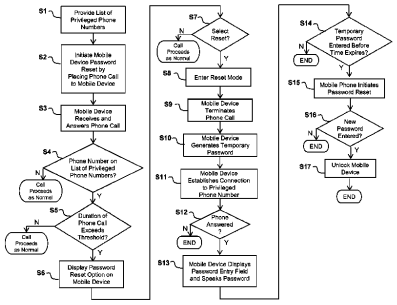
(Continued)

Primary Examiner — Kashif Siddiqui
Assistant Examiner — Ather Mohiuddin
(74) *Attorney, Agent, or Firm* — Dan Simek; Hoffman Warnick LLC

(57) **ABSTRACT**

The disclosure is directed to a device password reset. A method in accordance with an embodiment includes: receiving a phone call at a locked mobile device from a phone having a privileged phone number; initiating a password reset in response to the receipt of the phone call from the privileged phone number and the phone call exceeding a predetermined time duration threshold by: terminating, by the locked mobile device, the phone call from the phone having the privileged phone number; generating, by the locked mobile device, a temporary password; establishing, by the locked mobile device, a connection to the phone having the privileged phone number; displaying, by the locked mobile device, a password entry field; communicating, by the locked mobile device, the temporary password via the connection to the phone having the privileged phone number; and unlocking the locked mobile device upon successful entry of the temporary password in the password entry field displayed by the locked mobile device.

20 Claims, 6 Drawing Sheets



(51) **Int. Cl.**

G06F 7/04	(2006.01)
H04W 12/08	(2009.01)
H04L 29/06	(2006.01)

(56) **References Cited**

U.S. PATENT DOCUMENTS

2014/0085048	A1*	3/2014	Hadizad	340/5.64
2014/0113593	A1*	4/2014	Zhou et al.	455/411

OTHER PUBLICATIONS

U.S. Appl. No. 14/020,937, Notice of Allowance Feb. 18, 2015, 8 pages.
U.S. Appl. No. 14/020,937, Non-Final Office Action Jan. 23, 2015, 13 pages.
Notice of Allowance and Fee(s) Due for U.S. Appl. No. 14/020,937, dated Feb. 18, 2015, 8 pages.

* cited by examiner

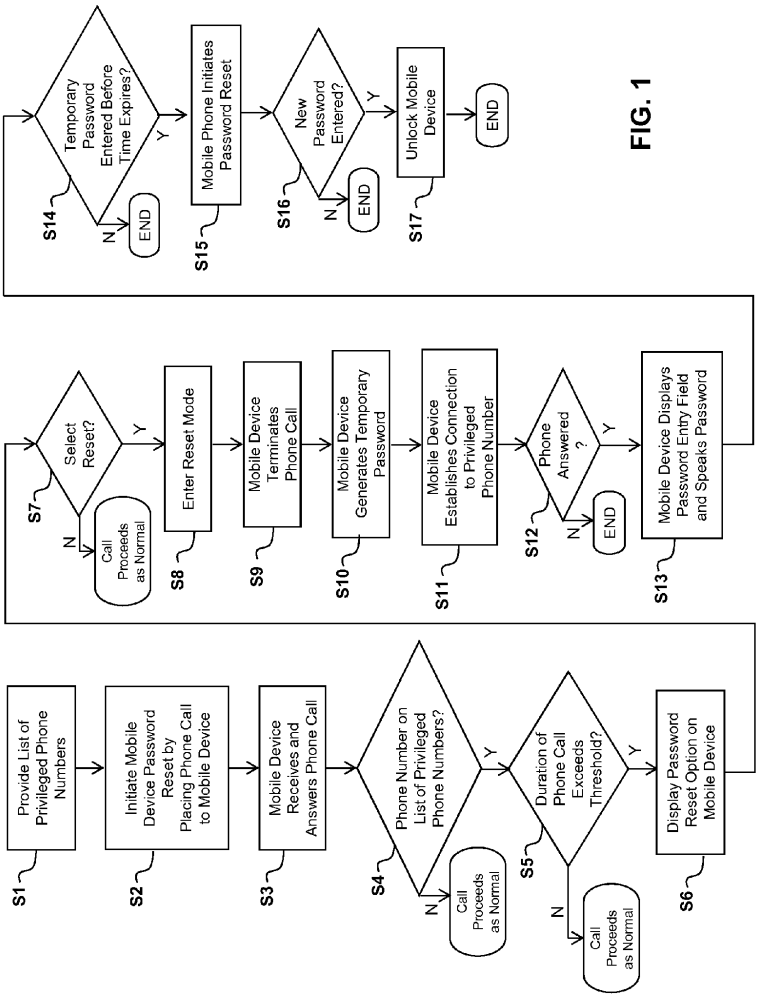

Provide List of Privileged Phone Numbers
S1
Initiate Mobile Device Password Reset by Placing Phone Call to Mobile Device
S2
Mobile Device Receives and Answers Phone Call
S3
Phone Number on List of Privileged Phone Numbers?
S4
Y
N
Call Proceeds as Normal
Duration of Phone Call Exceeds Threshold?
S5
Y
N
Call Proceeds as Normal
Display Password Reset Option on Mobile Device
S6
Select Reset?
S7
Y
N
Call Proceeds as Normal
Enter Reset Mode
S8
Mobile Device Terminates Phone Call
S9
Mobile Device Generates Temporary Password
S10
Mobile Device Establishes Connection to Privileged Phone Number
S11
Phone Answered ?
S12
Y
N
END
Mobile Device Displays Password Entry Field and Speaks Password
S13
Temporary Password Entered Before Time Expires?
S14
Y
N
END
Mobile Phone Initiates Password Reset
S15
New Password Entered?
S16
Y
N
END
Unlock Mobile Device
S17
END

FIG. 1

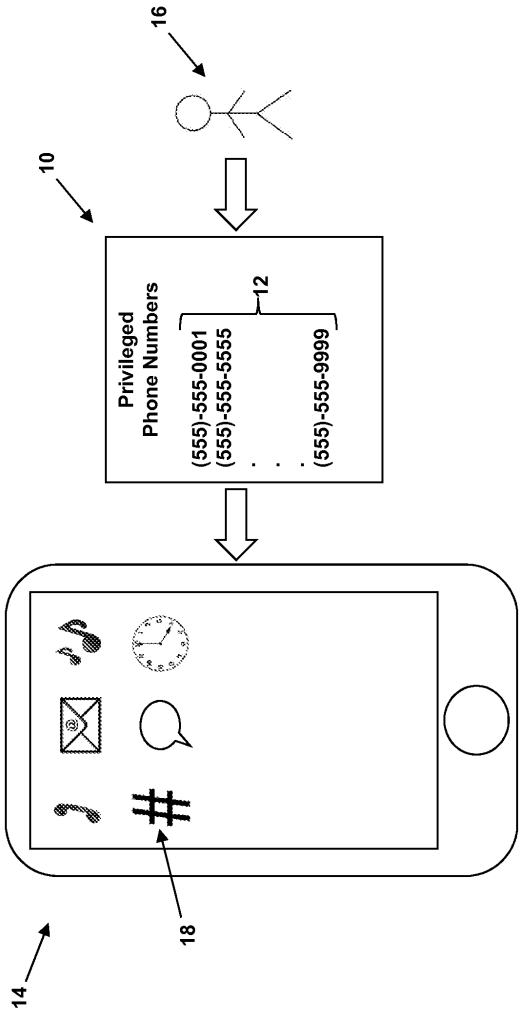

16
10
Privileged
Phone Numbers
12
(555)-555-0001
(555)-555-5555
. . .
(555)-555-9999
18
14

FIG. 2

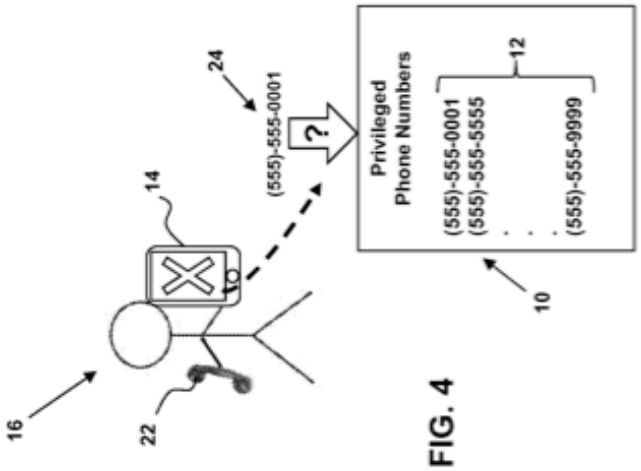

24
(555)-555-0001
?
Privileged
Phone Numbers
12
(555)-555-0001
(555)-555-5555
(555)-555-9999
10
14
16
22

FIG. 4

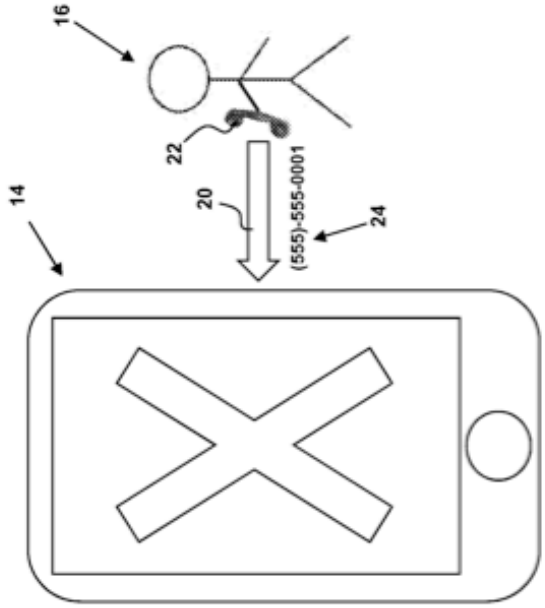

16
22
20
(555)-555-0001
24
14

FIG. 3

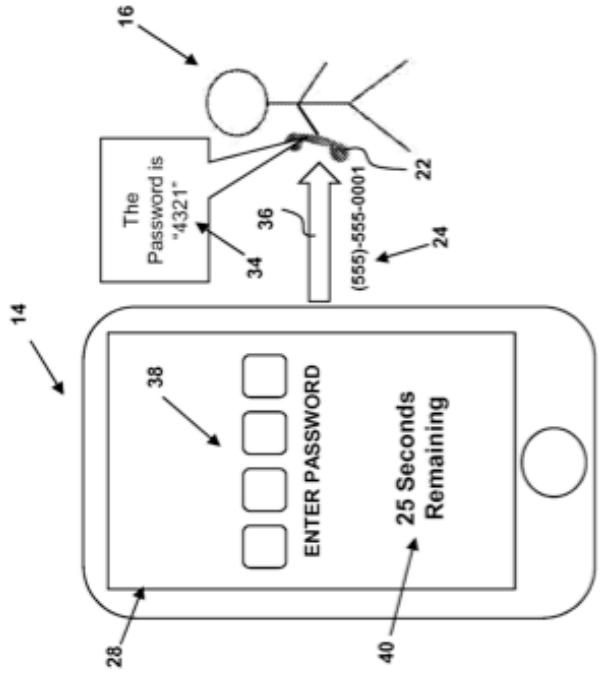

16
The Password is "4321"
34
36
(555)-555-0001
22
24
14
38
ENTER PASSWORD
25 Seconds Remaining
28
40

FIG. 6

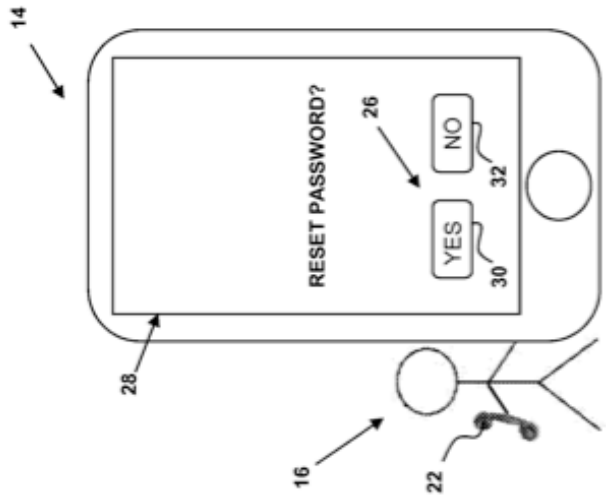

14
RESET PASSWORD?
26
NO
32
YES
30
28
16
22

FIG. 5

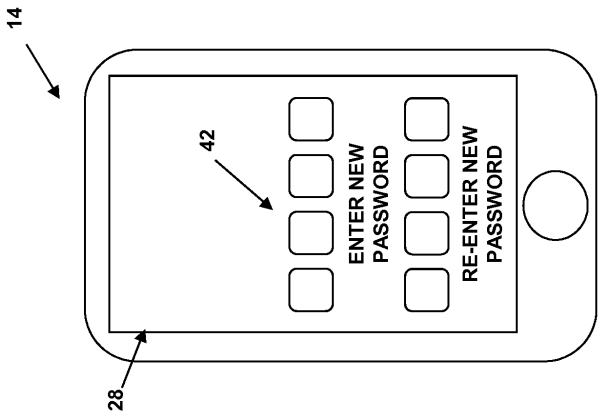


FIG. 7

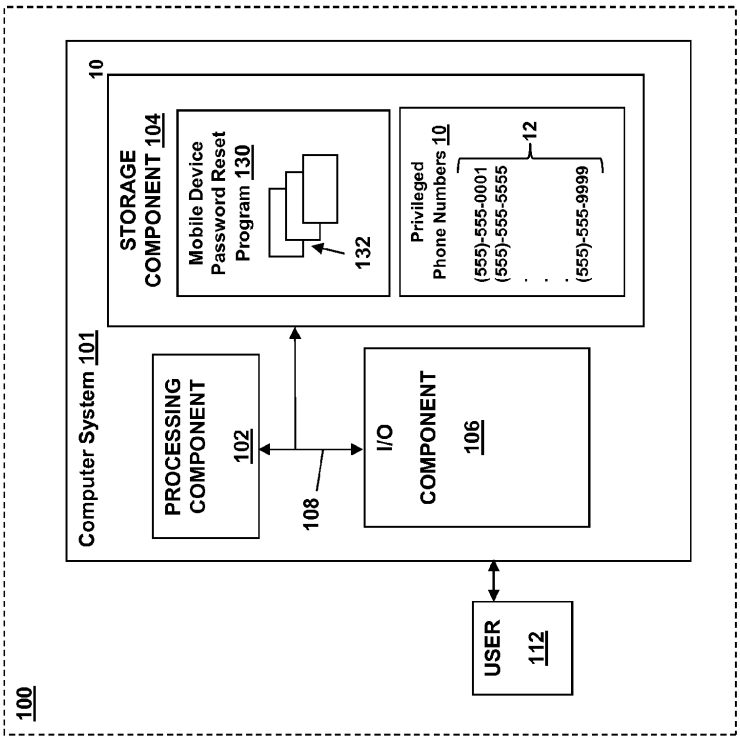

100
USER
112
Computer System 101
10
PROCESSING COMPONENT
102
108
I/O COMPONENT
106
STORAGE COMPONENT 104
Mobile Device Password Reset Program 130
132
Privileged Phone Numbers 10
12
(555)-555-0001
(555)-555-5555
(555)-555-9999

FIG. 8

MOBILE DEVICE PASSWORD RESET

REFERENCE TO PRIOR APPLICATIONS

The current application is a continuation application of U.S. Utility application Ser. No. 14/020,937, which was filed on 9 Sep. 2013, which is hereby incorporated by reference.

TECHNICAL FIELD

The present invention relates generally to mobile devices, and more particularly, to a mobile device password reset.

RELATED ART

Many methods are available for resetting a forgotten or lost password of a mobile device. One method, typically referred to as a master or factory reset, returns a mobile device to its original, default operating system state. However, this process erases all data (e.g., contacts, applications, personalized settings, etc.) added to the mobile device after purchase. Another method requires a phone call to the phone company that provides service to the mobile device. The present invention addresses these problems allowing users to avoid the data reconstruction of a hard reset and the cost of service provider involvement.

SUMMARY

A first aspect of the invention provides a device password reset method, comprising: receiving a phone call at a locked mobile device from a phone having a privileged phone number; initiating a password reset in response to the receipt of the phone call from the phone having the privileged phone number and the phone call exceeding a predetermined time duration threshold, the password reset comprising: terminating, by the locked mobile device, the phone call from the privileged phone number; generating, by the locked mobile device, a temporary password; establishing, by the locked mobile device, a connection to the phone having the privileged phone number; displaying, by the locked mobile device, a password entry field; communicating, by the locked mobile device, the temporary password via the connection to the phone having the privileged phone number; and unlocking the locked mobile device upon successful entry of the temporary password in the password entry field displayed by the locked mobile device.

A second aspect of the invention provides a device configured to perform a password reset method, the method comprising: receiving a phone call at a locked mobile device from a phone having a privileged phone number; initiating a password reset in response to the receipt of the phone call from the phone having the privileged phone number and the phone call exceeding a predetermined time duration threshold, the password reset comprising: terminating, by the locked mobile device, the phone call from the privileged phone number; generating, by the locked mobile device, a temporary password; establishing, by the locked mobile device, a connection to the phone having the privileged phone number; displaying, by the locked mobile device, a password entry field; communicating, by the locked mobile device, the temporary password via the connection to the phone having the privileged phone number; and unlocking the locked mobile device upon successful entry of the temporary password in the password entry field displayed by the locked mobile device.

A third aspect of the invention provides a computer program product including program code embodied in at least one computer-readable storage medium, which when executed, enables a computer system to implement a device password reset method, the method comprising: receiving a phone call at a locked mobile device from a phone having a privileged phone number; initiating a password reset in response to the receipt of the phone call from the phone having the privileged phone number and the phone call exceeding a predetermined time duration threshold, the password reset comprising: terminating, by the locked mobile device, the phone call from the privileged phone number; generating, by the locked mobile device, a temporary password; establishing, by the locked mobile device, a connection to the phone having the privileged phone number; displaying, by the locked mobile device, a password entry field; communicating, by the locked mobile device, the temporary password via the connection to the phone having the privileged phone number; and unlocking the locked mobile device upon successful entry of the temporary password in the password entry field displayed by the locked mobile device.

Other aspects of the invention provide methods, systems, program products, and methods of using and generating each, which include and/or implement some or all of the actions described herein. The illustrative aspects of the invention are designed to solve one or more of the problems herein described and/or one or more other problems not discussed.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other features of the disclosure will be more readily understood from the following detailed description of the various aspects of the invention taken in conjunction with the accompanying drawings that depict various aspects of the invention.

FIG. **1** shows a flow diagram of an illustrative process for a mobile device password reset, according to embodiments.

FIG. **2** depicts an illustrative setup process for a mobile device password reset, according to embodiments.

FIG. **3** depicts a user initiating a mobile device password reset by placing a phone call to a locked mobile device, according to embodiments.

FIG. **4** depicts a locked mobile device comparing the phone number of a received phone call to privileged phone numbers on a predefined list, according to embodiments.

FIG. **5** depicts the display of a password reset option to a user via a display of a mobile device, according to embodiments.

FIG. **6** depicts a mobile device placing a return phone call to the phone number of the phone that initiated a mobile device password reset, according to embodiments.

FIG. **7** depicts the initiation of a password reset upon receiving a correct temporary password, according to embodiments.

FIG. **8** shows an illustrative environment for a mobile device password reset according to an embodiment.

It is noted that the drawings may not be to scale. The drawings are intended to depict only typical aspects of the invention, and therefore should not be considered as limiting the scope of the invention. In the drawings, like numbering represents like elements between the drawings.

DETAILED DESCRIPTION

The present invention relates generally to mobile devices, and more particularly, to a mobile device password reset.

When a mobile device enters a locked state, operation of the mobile device may be prevented or severely limited. Such a locked state may occur automatically, for example, after a

predetermined period of inactivity, or may be activated manually (e.g., via buttons/keys on the mobile device or remotely over the Internet). Typically, the locked state of a mobile device is provided as a security measure to prevent unauthorized or unintended use of the mobile device. However, while in the locked state, most mobile devices allow incoming phone calls, which can be answered by a user of the mobile device, and/or a user of the mobile device may be able to place an outgoing emergency call.

To unlock a mobile device that has entered a locked state, a user typically enters a password into a password entry screen of the mobile device using a virtual or physical keypad of the mobile device. A password may comprise, for example, an alphanumeric passcode, passkey, passphrase, access code, personal identification number (PIN), a pattern entered on the screen, or other type of authentication data. If the user correctly enters the password within a predetermined number of attempts, the mobile device is unlocked and full functionality is restored. Repeated failures to enter the correct password may, in some cases, cause the mobile device to erase all data and perform a master reset.

The present invention provides a mobile device password reset that allows a user to securely regain full authorized access to a locked mobile device. In the present disclosure, such a mobile device may include, for example, a cell phone, smartphone, tablet computer, PDA, laptop computer, or other handheld computing/communication device capable of sending/receiving phone calls.

FIG. **1** shows a flow diagram of an illustrative process for a mobile device password reset according to embodiments. During a setup process S**1**, and as depicted in FIG. **2**, a predefined list **10** of one or more privileged phone numbers **12** is provided and stored in a mobile device **14** by an authorized user **16** (e.g., owner) of the mobile device **14**. For example, the predefined list **10** of privileged phone numbers **12** may include the home and work phone numbers of the user **16**, a friend's cell phone number, a relative's land-line phone number, etc.

The user **16** may provide the predefined list **10** of privileged phone numbers **12** during an initial or subsequent configuration of the settings of the mobile device **14**. Application software **18** loaded and running on the mobile device **14** may also be used to provide the predefined list **10** of privileged phone numbers **12** to the mobile device **14**.

At S**2**, assuming the mobile device **14** is in a locked state and the user **16** has forgotten the password for unlocking the mobile device **14**, the user **16** initiates a mobile device password reset by placing a phone call **20** (FIG. **3**) to the mobile device **14** from another phone **22**. The phone **22** can comprise any telecommunication device capable of sending/receiving phone calls, including a mobile device, a land-line phone, a computer with VoIP capabilities, and/or the like. At S**3**, the phone call **20** is received and answered by the mobile device **14**.

At S**4**, the mobile device **14** compares (FIG. **4**) the phone number **24** of the phone call **20** to the privileged phone numbers **12** on the predefined list **10**. The phone number **24** of the phone call **20** may be determined via caller ID or using any other suitable technique.

If the phone number **24** of the phone call **20** is not on the predefined list **10** of privileged phone numbers **12** (N at S**4**), the mobile device password reset process ends and the call proceeds as normal. If, however, the phone number **24** of the phone call **20** is on the predefined list **10** of privileged phone numbers **12** (Y at S**4**), flow passes to S**5**.

At S**5**, the elapsed duration of the phone call **20** is monitored by the mobile device **14**. If the elapsed duration of the phone call **20** exceeds a predetermined time threshold (e.g., 10-15 seconds) (Y at S**5**), indicating that the phone call **20** has a high likelihood of being legitimate, a password reset option **26** (FIG. **5**) is displayed to the user **16** at S**6** via a display **28** of the mobile device **14**. If the phone call **20** is terminated before the predetermined time threshold has been exceeded (N at S**5**), the mobile device password reset process ends and the call proceeds as normal. The duration of the phone call **20** will generally be shorter in the case that the mobile device **14** is lost/stolen. In such a case, the user **16** would realize the mobile device **14** has been compromised (e.g., based on who answered the mobile device **14**) and hang-up before the predetermined time threshold, thereby terminating the mobile device password reset process.

If the user **16** selects the password reset option **26** (Y at S**7**), the mobile device **14** enters a password reset mode at S**8**. If the user **16** does not select the password reset option **26** (N at S**7**), the mobile device password reset process ends and the call proceeds as normal. Selection of the password reset option **26** may be provided, for example, via YES and NO buttons **30**, **32**, respectively, or in any other suitable manner.

Upon entering the password reset mode at S**8**, the mobile device **14** terminates the phone call **20** at S**9**. Thereafter, at S**10**, the mobile device **14** generates a random, one-time, temporary password **34** (FIG. **6**).

At S**11**, and as shown in FIG. **6**, the mobile device **14** establishes a connection (e.g., via a return phone call **36**) to the phone number **24** of the phone **22** that initiated the mobile device password reset. If the return phone call **36** is not answered by the user **16** (N at S**12**) the mobile device password reset process ends. If the return phone call **36** is answered by the user **16** (Y at S**12**), the mobile device **14**, at S**13**, displays a password entry field **38** and speaks the temporary password **34** to the user **16** (e.g., using text-to-speech) one or more times for a predetermined period of time (e.g., 30 seconds). In other embodiments, the mobile device **14** may communicate the temporary password **34** to the user **16** in a non-vocal manner. For example, the mobile device **14** may communicate the temporary password **34** to the user **16** via a short message service (SMS) text message, an email, and/or the like.

If the user **16** does not enter the correct temporary password **34** into the displayed password entry field **38** within the predetermined period of time (N at S**14**), the mobile device password reset process ends. If the user **16** enters the correct temporary password **34** into the displayed password entry field **38** within the predetermined period of time (Y at S**14**), flow passes to S**15**. As depicted in FIG. **6**, a timer **40** may be displayed on the mobile device **14** to indicate the time remaining during which the user **16** can enter the correct temporary password **34** into the displayed password entry field **38**.

At S**15**, upon receiving the correct temporary password **34**, the mobile device **14** immediately initiates a password change process (FIG. **7**), after which the user **16** is required to enter a new password **42** into the mobile device **14**. After successful completion of the password change process (Y at S**16**), the mobile device **14** is unlocked at S**17** and is ready for use. If the password reset is not completed (N at S**16**), the mobile device **14** remains locked and the mobile device password reset process ends. In this case, the user **16** must return to S**2** to restart the mobile device password reset process.

An illustrative environment **100** for providing a mobile device password reset is shown in FIG. **8**. The environment **100** includes at least one computer system **101** and a mobile device password reset program **130** that can perform processes described herein in order to provide a mobile device

password reset in accordance with embodiments. The environment **100** may be provided, for example, within a mobile device **14**.

The computer system **101** is shown including a processing component **102** (e.g., one or more processors), a storage component **104** (e.g., a storage hierarchy), an input/output (I/O) component **106** (e.g., one or more I/O interfaces and/or devices), and a communications pathway **108**. In general, the processing component **102** executes program code, such as the mobile device password reset program **130**, which is at least partially fixed in the storage component **104**. While executing program code, the processing component **102** can process data, such as a list **10** of privileged phone numbers **12** and/or the like, which can result in reading and/or writing transformed data from/to the storage component **104** and/or the I/O component **106** for further processing. The pathway **108** provides a communications link between each of the components in the computer system **101**. The I/O component **106** can include one or more human I/O devices, which enable a human user **112** to interact with the computer system **101** and/or one or more communications devices to enable a system user **112** to communicate with the computer system **101** using any type of communications link. To this extent, the mobile device password reset program **130** can manage a set of interfaces (e.g., graphical user interface(s), application program interfaces, communication interface(s), and/or the like) that enable human and/or system users **112** to interact with the mobile device password reset program **130**. Furthermore, the mobile device password reset program **130** can manage (e.g., store, retrieve, create, manipulate, organize, present, etc.) the data, such as the list **10** of privileged phone numbers **12** and/or the like, using any solution.

The computer system **101** can include one or more general purpose computing articles of manufacture (e.g., computing devices) capable of executing program code, such as the mobile device password reset program **130**, installed thereon. As used herein, it is understood that "program code" means any collection of instructions, in any language, code or notation, that cause a computing device having an information processing capability to perform a particular action either directly or after any combination of the following: (a) conversion to another language, code or notation; (b) reproduction in a different material form; and/or (c) decompression. To this extent, the mobile device password reset program **130** can be embodied as any combination of system software and/or application software.

Furthermore, the mobile device password reset program **130** can be implemented using a set of modules **132**. In this case, a module **132** can enable the computer system **20** to perform a set of tasks used by the mobile device password reset program **130**, and can be separately developed and/or implemented apart from other portions of the mobile device password reset program **130**. As used herein, the term "component" means any configuration of hardware, with or without software, which implements the functionality described in conjunction therewith using any solution, while the term "module" means program code that enables a computer system **101** to implement the actions described in conjunction therewith using any solution. When fixed in a storage component **104** of a computer system **101** that includes a processing component **102**, a module is a portion of a component that implements the actions. Regardless, it is understood that two or more components, modules, and/or systems may share some/all of their respective hardware and/or software. Furthermore, it is understood that some of the functionality discussed herein may not be implemented or additional functionality may be included as part of the computer system **101**.

When the computer system **101** includes multiple computing devices, each computing device can have only a portion of the mobile device password reset program **130** fixed thereon (e.g., one or more modules **132**). However, it is understood that the computer system **101** and the mobile device password reset program **130** are only representative of various possible equivalent computer systems that may perform a process described herein. To this extent, in other embodiments, the functionality provided by the computer system **101** and the mobile device password reset program **130** can be at least partially implemented by one or more computing devices that include any combination of general and/or specific purpose hardware with or without program code. In each embodiment, the hardware and program code, if included, can be created using standard engineering and programming techniques, respectively.

When the computer system **101** includes multiple computing devices, the computing devices can communicate over any type of communications link. Furthermore, while performing a process described herein, the computer system **101** can communicate with one or more other computer systems using any type of communications link. In either case, the communications link can include any combination of various types of optical fiber, wired, and/or wireless links; include any combination of one or more types of networks; and/or utilize any combination of various types of transmission techniques and protocols.

While shown and described herein as a method and system for detecting illegal activity through interpersonal relationship resolution, it is understood that aspects of the invention further provide various alternative embodiments. For example, in one embodiment, the invention provides a computer program fixed in at least one computer-readable storage medium, which when executed, enables a computer system to for detect illegal activity through interpersonal relationship resolution. To this extent, the computer-readable storage medium includes program code, such as the mobile device password reset program **130**, which enables a computer system to implement some or all of a process described herein. It is understood that the term "computer-readable storage medium" includes one or more of any type of tangible medium of expression, now known or later developed, from which a copy of the program code can be perceived, reproduced, or otherwise communicated by a computing device. For example, the computer-readable medium can include: one or more portable storage articles of manufacture; one or more memory/storage components of a computing device; paper; and/or the like.

Another embodiment of the invention provides a method of providing a copy of program code, such as the mobile device password reset program **30**, which enables a computer system to implement some or all of a process described herein. In this case, a computer system can process a copy of the program code to generate and transmit, for reception at a second, distinct location, a set of data signals that has one or more of its characteristics set and/or changed in such a manner as to encode a copy of the program code in the set of data signals. Similarly, an embodiment of the invention provides a method of acquiring a copy of the program code, which includes a computer system receiving the set of data signals described herein, and translating the set of data signals into a copy of the computer program fixed in at least one computer-readable medium. In either case, the set of data signals can be transmitted/received using any type of communications link.

Still another embodiment of the invention provides a method for providing a mobile device password reset. In this case, a computer system, such as the computer system **101**,

can be obtained (e.g., created, maintained, made available, etc.) and one or more components for performing process(es) described herein can be obtained (e.g., created, purchased, used, modified, etc.) and deployed to the computer system. To this extent, the deployment can include one or more of: (1) installing program code on a computing device; (2) adding one or more computing and/or I/O devices to the computer system; (3) incorporating and/or modifying the computer system to enable it to perform a process described herein; and/or the like.

The foregoing description of various aspects of the invention has been presented for purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise form disclosed, and obviously, many modifications and variations are possible. Such modifications and variations that may be apparent to an individual skilled in the art are included within the scope of the invention as defined by the accompanying claims.

What is claimed is:

1. A password reset method, comprising:
- receiving a phone call at a locked mobile device from a phone having a privileged phone number;
- initiating a password reset in response to the receipt of the phone call from the phone having the privileged phone number and the phone call exceeding a predetermined time duration threshold;
- displaying a password reset option on the locked mobile device in response to the initiation of the password reset; and
- selecting the password reset option to perform the password reset, the password reset comprising:
  - terminating, by the locked mobile device, the phone call from the privileged phone number;
  - generating, by the locked mobile device, a temporary password;
  - establishing, by the locked mobile device, a connection to the phone having the privileged phone number;
  - displaying, by the locked mobile device, a password entry field;
  - communicating, by the locked mobile device, the temporary password via the connection to the phone having the privileged phone number; and
  - unlocking the locked mobile device upon successful entry of the temporary password in the password entry field displayed by the locked mobile device.

2. The password reset method of claim **1**, wherein the connection comprises a phone call.

3. The password reset method of claim **1**, wherein the connection comprises a text message.

4. The password reset method according to claim **1**, wherein the unlocking further comprises:
- initiating, by the mobile device, a timer when communicating the temporary password via the connection to the phone having the privileged phone number; and
- unlocking the locked mobile device upon successful entry of the temporary password in the displayed password entry field within a predetermined period of time as determined via the timer.

5. The password reset method according to claim **1**, wherein the unlocking further comprises:
- requesting, by the locked mobile device, a new password upon successful entry of the temporary password in the displayed password entry field; and
- unlocking the locked mobile device upon successful entry of the new password.

6. The password reset method according to claim **1**, wherein the communicating further comprises:
- speaking, by the locked mobile device, the temporary password during the connection.

7. The password reset method according to claim **1**, further comprising:
- storing at least one privileged phone number in the mobile device.

8. The password reset method according to claim **7**, wherein the initiating the password reset further comprises:
- comparing a phone number of the received phone call to each of the privileged phone numbers stored in the mobile device; and
- initiating the password reset when the phone number of the received phone call matches one of the privileged phone numbers stored in the mobile device.

9. A device configured to perform a password reset method, the method comprising:
- receiving a phone call at a locked mobile device from a phone having a privileged phone number;
- initiating a password reset in response to the receipt of the phone call from the phone having the privileged phone number and the phone call exceeding a predetermined time duration threshold;
- displaying a password reset option on the locked mobile device in response to the initiation of the password reset; and
- selecting the password reset option to perform the password reset, the password reset comprising:
  - terminating, by the locked mobile device, the phone call from the privileged phone number;
  - generating, by the locked mobile device, a temporary password;
  - establishing, by the locked mobile device, a connection to the phone having the privileged phone number;
  - displaying, by the locked mobile device, a password entry field;
  - communicating, by the locked mobile device, the temporary password via the connection to the phone having the privileged phone number; and
  - unlocking the locked mobile device upon successful entry of the temporary password in the password entry field displayed by the locked mobile device.

10. The device of claim **9**, wherein the connection comprises a phone call.

11. The device of claim **9**, wherein the connection comprises a text message.

12. The device according to claim **9**, wherein the unlocking further comprises:
- initiating, by the mobile device, a timer when communicating the temporary password via the connection to the phone having the privileged phone number; and
- unlocking the locked mobile device upon successful entry of the temporary password in the displayed password entry field within a predetermined period of time as determined via the timer.

13. The device according to claim **9**, wherein the unlocking further comprises:
- requesting, by the locked mobile device, a new password upon successful entry of the temporary password in the displayed password entry field; and
- unlocking the locked mobile device upon successful entry of the new password.

14. The device according to claim **9**, wherein the communicating further comprises:
- speaking, by the locked mobile device, the temporary password during the connection.

15. The device according to claim **9**, the method further comprising:

storing at least one privileged phone number in the mobile device.

16. The device according to claim **15**, wherein the initiating the password reset further comprises:

comparing a phone number of the received phone call to each of the privileged phone numbers stored in the mobile device; and

initiating the password reset when the phone number of the received phone call matches one of the privileged phone numbers stored in the mobile device.

17. A computer program product comprising program code embodied in at least one non-transitory computer-readable storage medium, which when executed, enables a computer system to implement a device password reset method, the method comprising:

receiving a phone call at a locked mobile device from a phone having a privileged phone number;

initiating a password reset in response to the receipt of the phone call from the phone having the privileged phone number and the phone call exceeding a predetermined time duration threshold;

displaying a password reset option on the locked mobile device in response to the initiation of the password reset; and

selecting the password reset option to perform the password reset, the password reset comprising:

terminating, by the locked mobile device, the phone call from the privileged phone number;

generating, by the locked mobile device, a temporary password;

establishing, by the locked mobile device, a connection to the phone having the privileged phone number;

displaying, by the locked mobile device, a password entry field;

communicating, by the locked mobile device, the temporary password via the connection to the phone having the privileged phone number; and

unlocking the locked mobile device upon successful entry of the temporary password in the password entry field displayed by the locked mobile device.

18. The computer program product of claim **17**, wherein the connection comprises a phone call, a text message, or an email.

19. The computer program product of claim **17**, wherein the unlocking further comprises:

initiating, by the mobile device, a timer when communicating the temporary password via the connection to the phone having the privileged phone number; and

unlocking the locked mobile device upon successful entry of the temporary password in the displayed password entry field within a predetermined period of time as determined via the timer.

20. The computer program product of claim **17**, wherein the unlocking further comprises:

requesting, by the locked mobile device, a new password upon successful entry of the temporary password in the displayed password entry field; and

unlocking the locked mobile device upon successful entry of the new password.

* * * * *